Guide de sécurité Windows NT

Réflexions & Conseils pour configurer de manière sécurisée Windows NT dans des environnements hétérogènes.

Une étude pour

NSA Research

par

Trusted Systems Services

ntguide@trustedsystems.com

http://www.trustedsystems.com

217-344-0996

14 Septembre 1998

Auteur: **Steve Sutton** *Trusted Systems Services*

Sponsor: **Scott Cothrell** *National Security Agency*

Adaptation Française:

Ali Nedjimi *Ecole Supérieure d'Informatique*

Table des matières

Nouveautés dans cette édition

Cette édition suit celle datée du 18 Mars 1998 et contient quelques petites corrections typographiques. Elle contient aussi une révision de la section “Restreindre l’accès à distance de la base de registre” qui inclut des sujets de discussion qui se trouvent maintenant dans “Accès distant anonyme à la base de registre.” Cette partie comportait quelques inexactitudes significatives, et les lecteurs devraient regarder les corrections.

1. Introduction

Cette recherche sur la sécurisation du système d'exploitation Windows NT™ de Microsoft a été menée par Trusted Systems Services, Inc., sous contrat avec la National Security Agency (MDA904-97-C-0336). Le but était de résumer l'état de l'art concernant la configuration sécurisée de Windows NT Server et Workstation 4.0, basé sur un vaste examen des travaux publiés, pour offrir un guide à la fois pour le gouvernement et les utilisateurs commerciaux. Ce contrat incluait aussi le développement d'un utilitaire programmable connu sous le nom de code "Checker" pour vérifier et renforcer les stratégies de sécurité [1].Voir "Logiciel Checker " plus bas pour une description détaillée du prototype du logiciel.

Portée et Intentions

Ces méthodes décrivent les pratiques qui permettent de contrer les attaques les plus communément utilisées sur les installations des réseaux Windows NT qui exposent ?? les données utilisateurs à des modifications malveillantes. Le but est de rendre Windows NT aussi sécurisé qu'il puisse *raisonnablement et pratiquement l'être.* Nous croyons que ces méthodes réduisent les risques de sécurité à un niveau d'égalité avec les attaques actuellement utilisées. Le même genre de menaces existe dans les environnements gouvernementaux et commerciaux et les techniques pour les contenir sont les mêmes ici. Ce guide est applicable à presque tous les environnements Windows NT, il est le résultat d'un vaste examen des travaux publiés concernant la sécurité sur Windows NT et il est donc en accord avec plusieurs travaux majeurs précédents et plus particulièrement [Sutt96], [Maye96], [Micr97], [TFM], and [Navy97]. (Les éléments entre "[…]" se réfèrent à des documents définis dans la section *Références* à la fin du guide.)

Windows NT a de nombreux moyens de renforcer sa sécurité. Toutefois, même dans le mode le plus sécurisé que ce guide aborde, nous ne recommandons pas le paramètre le plus restrictif pour chaque contrôle. La compréhension que ces recommandations doivent être à la fois efficaces contre certaines menaces mais aussi pratiques est implicite. Certains contrôles entravent la capacité opérationnelle et leur utilisation doit être soigneusement pensée et équilibrée par rapport à la sécurité qu'ils offrent.

La sécurité contre les intrusions actives est un phénomène à "maillon faible". Une philosophie serait de résoudre en premier lieu les problèmes de sécurité majeurs même si cela implique de laisser les moins importants tels qu'ils le sont. Avec cette philosophie, l'on ramène les risques pratiquement au même niveau en réduisant les majeurs, tout en laissant les mineurs inchangés. Une autre philosophie réduit *tous* les risques à leur valeur la plus faible en essayant d'équilibrer ces deux extrêmes. Ainsi, notre guide recommande des méthodes qui ont les effets les plus importants en réduisant les risques globaux et qui laissent la résolution des problèmes mineurs comme optionnelle. Enfin, les contrôles que vous mettez en place dépendent des risques présents sur votre site, et il serait conseillé d'utiliser toutes les vérifications de sécurité nécessaires, y compris celles qui peuvent sembler mineures, si elles peuvent contrer une menace légitime.

Certaines de nos recommandations sont directes, alors que d'autres nécessitent une évaluation considérable de la part des administrateurs, et pour le dernier chapitre nous présentons une brève discussion sur les critères essentiels pris en compte. Bien que ce document inclut

[1] Vérifiez la disponibilité de Checker sur le site de Trusted Systems Services (http://www.TrustedSystems.com).

certaines présentations ou introductions synthétiques, il ne constitue pas un didacticiel ou un manuel administratif. Nous supposons que les administrateurs qui mettent en œuvre ce guide sont familiers avec les manuels d'administration qui accompagnent Windows NT et sont compétents dans la gestion de sa sécurité. La section *Références* à la fin de ce guide contient un certain nombre de lectures didacticiels.

Windows NT a été classé comme C2 sous l' U.S. *Trusted Computer Systems Evaluation Criteria* (TCSEC, or "Orange Book") et classé de manière analogue par son équivalent Européen appelé l'ITSEC. Ces classements fournissent l'assurance que l'architecture de base de Windows NT a été mise en place de manière rationnelle. Malheureusement ces critères ne présentent pas comment le configurer et l'utiliser de façon sécurisée.

Enfin, ces recommandations ne constituent pas la politique de la NSA. Elles sont présentées ici comme l'état de l'art sur la configuration de la sécurité de Windows NT, et sont ouvertes à l'interprétation et à la modification pour convenir aux risques d'un site particulier. Ces recommandations représentent un essai de documentation de "la meilleure pratique commerciale" pour configurer Windows NT de manière sécurisée.

Nous considérons ce guide comme un document actif, et volontiers ouvert à la discussion et aux réponses de la part de ses lecteurs. Il y a sans aucun doute des parties qui peuvent être améliorées grâce à ce processus.

Envoyez vos commentaires à ntguide@trustedsystems.com.

Niveau 1 & Niveau 2

Nous définissons deux niveaux de sécurité niveau 1 et niveau 2 où le niveau 2 est plus sécurisé que le niveau 1 :

Niveau 1 : il s'agit d'une modeste amélioration d'une installation Windows NT standard. Virtuellement tous les sites qui estiment la sécurité importante devraient implémenter le Niveau 1.

Niveau 2 : il s'applique à des sites ayant un souci considérable de sécurité – ceux qui veulent étendre les protections que Windows NT fournit.

L'implémentation du Niveau 2 avec toutes ses recommandations et options vous permet d'être compétitif face aux efforts d'intrusions et d'attaques. Toutefois le Niveau 2 requiert *considérablement* plus d'efforts pour le mettre en place et le maintenir que le Niveau 1 et ne devrait pas être utilisé à la légère.

☞ Les pratiques nécessaires pour un niveau donné sont simplement notées comme "**prescrites**." Les autres pratiques sont "**recommandées**," et il est implicite qu'elles soient *hautement recommandées* pour le Niveau 2

En pratique, peu de sites seront exclusivement Niveau 1 ou Niveau 2 mais seront plutôt un mélange des différentes pratiques pour répondre au mieux à la situation. Notre but n'est **pas** d'établir un critère de classement, le Niveau 1 et le Niveau 2 sont des désignations de travail que nous n'avons pas l'intention d'accorder de quelque façon que ce soit. Par exemple si vous décidez de ne pas implémenter quelques recommandations mineures du Niveau 2 alors que le reste l'est, nous n'avons pas l'intention que quelqu'un puisse désigner votre système comme "Non conforme Niveau 2".

Structure

Chaque chapitre contient une ou plusieurs sections *Conseils* qui liste succinctement les actions recommandées . Une section *Notes* qui suit généralement le chapitre contient des notions importantes et des descriptions plus détaillées des techniques . Une section référence à la fin d'un chapitre liste les œuvres et documents liés au sujet.

Il est implicite que toutes les recommandations doivent être revues et adaptées régulièrement. Les notes contenues dans les sections intitulées *Examen Régulier* (là où elles sont présentes) à l'intérieur du Guide présentent seulement des suggestions particulières ou détaillées pour ces examens. Nous ne prescrivons pas de délai de révision spécifique, les sites de Niveau 1 devrait les réviser tous les 3-6 mois, et ceux de Niveau 2 tous les 1-2 mois.

Notes & Terminologie

La plupart des conseils peuvent être mis en place avec des outils fournis avec Windows NT. Certaines actions suggérées nécessitent des outils fournis par des sociétés tierces, bien que nous n'en mentionnons que peu. Lorsque l'on souligne ces outils, nous ne manifestons pas d'adhésion particulière; nous ne disons pas qu'ils sont les seul outils de ce type pour une tache particulière ou les meilleurs. Plus précisément , notre idée générale est que si nos lecteurs connaissent le nom d'un outil, ils peuvent le chercher sur Internet pour trouver des produits similaires.

Ce guide ne traite pas des "dénies of service". Que l'on considère ces derniers comme des problèmes de "sécurité" à proprement dits ou pas, les solutions sont issues plus de la science que de la sécurité. Nous ne prescrivons pas de sauvegardes régulières et de procédures de restauration, bien qu'elles puissent être vitales pour se remettre d'une intrusion.

Le guide couvre Windows NT 4.0 et inclut le Service Pack 3.

Nous utilisons le terme "administrateur" de manière générique.

Le logiciel Checker

Ce contrat incluait aussi le développement d'un logiciel prototype connu sous le nom de code "Checker" pour examiner et renforcer les stratégies de sécurité Windows NT. Checker est un utilitaire configurable en ligne de commande qui examine et dans certains cas corrige, de nombreux attributs de sécurité de Windows NT Server ou Workstation. Checker vous permet de créer des scripts simples en tant que fichiers texte utilisables sur n'importe quel éditeur de texte. Vous lancez alors le programme CHECKER.EXE qui lit le script et exécute des examens de sécurité. Le format du script est appelé le "Langage Checker ", un langage de script simple.

Checker version 1.0 est un prototype développé sous ce contrat. Le but du prototype Checker était d'en démontrer la faisabilité, et il peut y avoir encore beaucoup d'améliorations. Trusted Systems améliore actuellement le Checker avec des fonctions commerciales.

Checker peut examiner les paramètres de sécurité suivants:

- Les **ACLs** (Access Control Lists = Listes de Contrôles d'accès) des fichiers et des répertoires sur des systèmes de fichiers NTFS et les clés de la base de registres. Vous pouvez spécifier l' ACL en utilisant une simple chaîne de texte, par exemple les 3 entrées suivantes :

```
"JJones:Lire  everyone:full  TRSYS\PPost:rwxd/rw"
```

- Les **SACLs (Listes de Contrôles d'accès de Sécurité) d'Audit** (les flags d'audit des objets) des fichiers et répertoires sur des systèmes de fichiers NTFS et les clés de la base de registres.
- **Valeurs de la base de registres**, par exemple: (1) que certaines clés ou leurs valeurs existent (ou n'existent pas), (2) qu'une valeur DWORD (numérique) soit plus grande (plus petite que , etc.) qu'un nombre dans une certaine plage ou une liste de valeurs, et (3) des tests analogues sur des chaînes du Registre. Si un test échoue, vous pouvez demander à Checker d'en modifier la valeur.[2]
- La stratégie d'**Audit** du gestionnaire des utilisateurs , notamment le fait que la fonction d'audit soit activée ou non et les catégories sélectionnées pour un succès/échec de l'audit.
- La **Stratégie des Droits** du gestionnaire des utilisateurs, testant les relations entre un droit et ses utilisateurs et groupes, ou un utilisateur ou un groupe et ses droits. Par exemple vous pouvez vérifier qu'un utilisateur possède au plus certains Droits, ou qu'un Droit exclut certains utilisateurs.
- La **Stratégie des comptes** du gestionnaire d'utilisateur, qui vous permet de vous assurez que par exemple un mot de passe fasse une certaine longueur et qu'il ait une certaine durée de vie.
- Les **Comptes d'utilisateurs individuels**, par exemple, que le compte soit désactivé ou que l'utilisateur puisse être autorisé à modifier le mot de passe de son compte. Vous pouvez vérifier tous les comptes ou en exclure une certaine partie donnée.

Votre script peut demander au Checker d'afficher des messages de réussite ou d'erreur. Vous pouvez utiliser les messages par défaut du Checker, définir les votres, ou utiliser les deux. Les messages peuvent être envoyés vers deux endroits logiques : Warning et Log. Le principe général est que les avertissements sont urgents et les enregistrements beaucoup moins, mais bien évidemment vous pouvez les utiliser quand vous le voulez. Vous pouvez diriger l'un ou l'autre des types de messages vers la sortie standard ou d'erreur de la commande, ou vers un fichier. Vous pouvez designer des destinations "normales" pour à la fois les avertissements et les enregistrements dans votre script, et ensuite diriger les messages issus de contrôles spécifiques vers d'autres destinations.

Un script Checker est un simple fichier texte que vous pouvez créer avec n'importe quel éditeur de texte. L'exemple suivant montre beaucoup de ses capacités. Checker permet les commentaires commençants avec "**//**" en fin de ligne, et nous les utilisons souvent ici pour expliquer les exemples.

```
AUDIT_POLICY
    RECORDING ON                                    // check that auditing is turned  on
      WARN TO DailyLog.txt FAILURE MESSAGE "You better turn that auditing on!"
      // could issue custom message like this in all the following examples
      // … otherwise we get Checker's standard message
```

[2] Le prototype Checker ne peut actuellement modifier que des valeurs de registre DWORD.

```
    CATEGORIES SUCCESS INCLUDES    system  logon
               FAILURE LIMITEDTO   tracking policy accountmgmt
```

```
RIGHTS_POLICY
    RIGHT InteractiveLogonRight                  // this Right (could list several)
        LIMITEDTO (  Administrators             // is limited to these 3 users/groups
                   "Opérateurs de Serveur"
                    TRSYS\JJones )

    ACCOUNT       ( Everyone "Authenticated Users")  // these 2 groups must have
        INCLUDES  (  InteractiveLogonRight          // … these 2 Rights
                     NetworkLogonRight     )
```

```
ACCOUNT_POLICY
     FORCE_LOGOFF      != forever
     PASSWORD_HISTORY  =  24
     MIN_PASSWORD_AGE  >   4             // days
     MAX_PASSWORD_AGE  <= 90             // days
     LOCKOUT_DURATION  INRANGE 10 TO 20  // minutes
     LOCKOUT_HEALING   >  30             // minutes
     LOCKOUT_THRESHOLD >=  6
```

```
ACCOUNTS
     USERS ( TRSYS\JJones  TRSYS\PPost )      // check two accounts
        NOT PASSWORD_EXPIRED
        NOT DISABLED
            PASSWORD_REQUIRED
        PASSWORD_AGE <=  90                   // days
        LAST_LOGON   <= 180                   // days
        WORKSTATIONS
          ( apple carrot pear )               // "allowed workstation" list

    USERS ALL EXCEPT ( TRSYS/Administrators ) // check all accounts except this one
       NOT USER_MAY_MODIFIER_PASSWORD
```

```
NTFS_ACL
     ACL   ( Everyone:LIRE              // an ACL with 3 entries
             JJones:Modifier
             TYRSYS\ProjectX:RWX/RX )
         wholêtree                      // one of several directory tree search options
           C:\GROUPS\PROJECTX           // a potentially long list of files/dirs
           C:\DATACACHE\

    // can also check Registry ACL's, and NTFS & Registry Audit SACL's
```

```
REGISTRY_VALUES
    KEY    HKLM\Software\Circus            EXISTS
    DWORD  HKLM\Software\Circus\Rings      =   3
    DWORD  HKLM\Software\Circus\TentSize   >= 42
    DWORD  HKLM\Software\Circus\Dates      INLIST ( 2 13 24 30 )
    DWORD  HKLM\Software\Circus\Horses     INRANGE 10 TO 15
                                              SET 12          // set to 12 on failure
    STRINGLIST  HKLM\Software\Circus\Animals
         INCLUDES ( "horses" "elephants" "tigers" ) NOCASE
```

Remerciements

De nombreux remerciement à nos relecteurs : Scott Cothrell, Chris Shutters, Tom Goss, Jack Lehman et Jean-Luc Moureaux pour l'adaptation française. Merci aussi à Alan Ramsbottom de ALS International Ltd. et Paul Ashton de Eigen Solutions pour leurs importantes relectures de ce document, et leurs nombreuses suggestions.

Ali NEDJIMI, auteur de l'adaptation Française du Guide, est MCP et spécialisé dans les architectures réseau NT. Il prépare un Diplôme d'ingénierie à l'Ecole Supérieure d'informatique de Paris (www.supinfo.com).

2. Vue d'ensemble du Guide

Ce qui suit est une vue d'ensemble des principaux chapitres du Guide:

3. Installation

Ce court mais important chapitre traite de problèmes matériels et du processus d'installation.

4. Domaines & Restrictions d'accès

Ce chapitre général explique comment utiliser les trois fonctions fondamentales qui déterminent quels utilisateurs peuvent se connecter sur les ordinateurs du réseau et s'ils peuvent le faire à distance:

- **Domaines & Approbation**: La définition du domaine et les relations d'approbation déterminent fondamentalement l'accès au réseau de l'utilisateur. Les "Comptes Correspondants" peuvent être utilisés pour garder des relations d'approbation simples.
- **Droits de connexion**: Le Droit de se connecter localement et le Droit de se connecter à distance à partir d'endroits différents sont définis dans la Stratégie de Droits de l'ordinateur et protègent ce dernier.
- **Restrictions par compte**: Chaque compte peut avoir une liste d'ordinateurs qui limitent le fait de se connecter localement, bien cela n'empêche pas l'accès a distance.

L'études de ces fonctions et de leurs combinaisons est fondamentale pour sécuriser un réseau Windows NT .

5. Structure Administrative

Ce chapitre traite de la configuration et de l'utilisation de comptes administrateurs et opérateurs. Il ne recommande pas une reconfiguration majeure des comptes standards Windows NT , mais offre des conseils sur la portée et l'assignation des comptes au personnel administratif.

- **Le compte "Administrateur":** Sur chaque ordinateur il y a un compte généré automatiquement appelé initialement "Administrateur" qui est tout-puissant et ne peut être effacé. Au moment de l'installation, c'est le seul compte administrateur de ce type. Nos recommandations préconisent de l'utiliser comme un compte de maintenance de dernier ressort, il vaut mieux se fier à un compte administrateur sur le domaine quand ses capacités sont nécessaires.
- **Administrateurs**: Ce guide présente les autres comptes tout-puissants, administrateurs "totaux" – comptes qui sont membres du groupe local "Administrateurs", ainsi que le groupe "Administrateur de domaine ". Ce guide suit généralement les pratiques standards de Windows NT. Le Niveau 2 sépare les administrateurs de stations de travail de ceux qui administrent des contrôleurs de domaine plus sensibles et les serveurs réseau importants. Cette section présente aussi des recommandations concernant la sécurité de l'utilisation de comptes administratifs.
- **Opérateur de domaine & Utilisateurs avec Pouvoirs**: Ce guide préconise l'utilisation intensive des groupes standards Windows NT "opérateurs" (y compris le groupe 'Utilisateurs avec pouvoirs' des Workstations) pour recourir le moins possible à l'emploi des comptes administratifs globaux. Il ne recommande aucune

modification significative pour les capacités de ces groupes. Il présente des possibilités quant à l'utilisation d'un groupe d'Utilisateurs avec Pouvoirs sur le Domaine pour une administration globale des Workstations ainsi que des conseils pour séparer les rôles critiques de sauvegarde et de restauration.

6. Politiques générales

Ce guide contient une grande variété de divers mais important contrôles de sécurité NT. Alors qu'ils peuvent sembler quelquefois obscurs, ils posent des questions auxquelles vous devriez répondre très tôt dans la mise en place de votre politique de sécurité.

7. Système de fichiers & paramètres d'ACL

Ce guide présente une stratégie pour affiner l'Access Control List (ACL) sur des objets systèmes sensibles, principalement ceux situés à la racine du système (habituellement C:\WINNT) qui contient les fichiers les plus sensibles sous Windows NT, ainsi que la base de registres NT. C'est par souci de simplification d'utilisation et de compatibilité logicielle que, par défaut, ces ACLs ne sont pas aussi strictes qu'elles pourraient l'être.

En général, différentes zones qui donnent aux utilisateurs la capacité de créer de nouveaux objets ou de modifier des objets fournis sont remplacées par des entrées qui leurs donnent le droit de lecture. Un nouveau groupe "Installateurs d'applications" se voit plutôt donné le droit de créer ou modifier ces objets. Les membres "Installateurs d'applications" sont des utilisateurs en qui on a confiance pour déterminer et installer les nouvelles applications sur le système, ce qui est la raison majeure pour laquelle ces utilisateurs ont besoin d'un droit d'écriture sur ces zones. Bien que les ACLs soient identiques tant pour le Niveau 1 que pour le Niveau 2, le critère de confiance pour être membre de ce groupe est substantiellement plus élevée au Niveau 2.

8. Applications & Répertoires Personnels

Ce guide présente une technique standard pour configurer les répertoires d'applications communs (programme) pour rendre ces composants systèmes sensibles résistants aux attaques comme les virus. Il préconise aussi d'enlever aux administrateurs critiques l'accès à de tels programmes à moins que les programmes soient totalement dignes de confiance. Ce guide décrit aussi une technique répandue de configuration ACLs sur les répertoires personnels, y compris les répertoires qui doivent être partagés par plusieurs utilisateurs ou groupes.

9. Comptes Utilisateur & Groupes

Ce guide donne quelques considérations pour les paramètres de comptes autres que les mots de passe. Par exemple, au Niveau 2 ce guide préconise une utilisation agressive des restrictions de comptes au niveau du choix des ordinateurs à partir desquels l'on peut se connecter localement. Ce guide couvre aussi des groupes d'utilisateurs autres que les comptes administratifs et les groupes usuels tels que Utilisateurs et Utilisateurs du Domaine.

10. Mots de passe

Ce guide prescrit l'utilisation totale et agressive des verrouillages de comptes et autres paramètres des mots de passe dans la Stratégie de compte. Il présente aussi plusieurs schémas communs et les classe en fonction de la probabilité de réussite d'une attaque basée sur les différents critères de mot de passe de Windows NT. Finalement chaque site doit choisir un schéma de mot de passe à la mesure de ses propres risques, ce guide offre les recommandations correspondantes.

11. Fichiers de Stratégie Système

Les Stratégies Systèmes sont des fonctions de Windows NT (et Windows 95) qui permettent aux administrateurs de contrôler de manière centralisée l'apparence de base du bureau de l'utilisateur. Ceci inclut différents aspects du menu démarrer, les éléments sur le bureau, le fait que le système montre ou pas une fenêtre "à usage limité" pendant la connexion... Les administrateurs peuvent configurer des stratégies centrales qui s'appliquent aux différents groupes d'utilisateurs et aux stations de travail. Au Niveau 2, ce guide recommande de configurer un fichier de stratégie de base simple, même si relativement peu de stratégies système soient de force significative au niveau sécurité.

12. Droits Utilisateurs

Chaque ordinateur Windows NT possède une stratégie de droit administrativement contrôlée qui attribue des combinaisons d'environ 30 "Droits" à des utilisateurs et groupes variés qui ont accès à cet ordinateur. Par exemple, la capacité de régler l'heure et la date est un droit. Quand elle est installée, la stratégie de droits Windows NT est limitée. Ce guide recommande quelques petites modifications pour renforcer la sécurité.

13. Stratégie d'audit & Journal de Sécurité

Le journal de sécurité de Windows NT peut collecter de manière détaillée une grande variété d'événements de sécurité pertinents dans des fichiers organisés, et les Administrateurs ont une considérable latitude concernant les événements qui sont enregistrés. Ce guide suggère les catégories de base à enregistrer pour chacun des Niveaux et la façon d'administrer le journal de sécurité Windows NT. Il s'agit d'un point de départ ouvert à de vastes interprétations en fonction des sites.

14. Services Systèmes

Les services systèmes de Windows NT sont des composants importants. Ce sont des programmes (souvent puissants) qui exécutent des fonctions de manière transparente pour les programmes des utilisateurs sur le réseau ou pour les éléments distants. Ce guide présente certaines recommandations afin d'éliminer les services inutiles ainsi que des suggestions pour utiliser des services sous des comptes plus sécurisés que ceux utilisés habituellement, notamment le tout puissant compte SYSTEM.

15. Partages

Ce court chapitre contient des recommandations pour créer des répertoires et des imprimantes partagées sur le réseau, ainsi que des commentaires sur "les partages administratifs cachés."

16. Réseau

Beaucoup de ces recommandations présentent les problèmes de sécurité dans des environnements basés sur des domaines Windows NT. Cette partie vous donne quelques conseils de base pour minimiser les services réseaux, enlever les éléments potentiellement dangereux d'un réseau Windows NT, isoler les services de partage natifs de Windows NT d'un intranet, et des conseils généraux sur la nécessité d'un firewall ou du cryptage.

17. Service d'accès distant (RAS)

RAS est un service natif de Windows NT qui permet aux ordinateurs de se connecter à des réseaux distants via un serveur Windows NT RAS. Cet accès se fait via une ligne téléphonique ou , (en utilisant le protocole PPTP) un intranet. Ce guide présente des réglages pour les paramètres de sécurité, peu nombreux ,de RAS pour les sites dont la politique permet l'accès distant.

18. Spoofing

Le Spoofing est le fait qu'un utilisateur malintentionné essaie de leurrer un utilisateur insouciant en lui faisant lancer un programme malveillant qu'il a crée. S'il réussit, le programme en question s'exécute avec toutes les capacités de l'utilisateur dupé et peut provoquer de vastes dommages si l'utilisateur est un administrateur. Le spoofing est peut être la menace la plus pernicieuse pour les systèmes d'exploitation. Malheureusement il est aussi difficile de le combattre car les contres mesures ont tendance à ne pas être spécifiques. Ce guide présente plusieurs menaces de spoofing et donne des conseils pour les minimiser.

19. Pratiques et Responsabilités de l'utilisateur

Ce chapitre présente les pratiques de bases que tous les utilisateurs devraient comprendre et utiliser. Il recommande que les administrateurs qui développent une stratégie de site avec de telles pratiques le fassent savoir aux utilisateurs du système.

3. Installation

Ces recommandations s'appliquent essentiellement à l'installation initiale d'un système Windows NT.

Conseils

Niveaux 1 & 2:

Désactiver le matériel inutile

- Enlevez les composants matériels que vous estimez dangereux (y compris les ports COM ou LPT), ou désactivez les à partir du BIOS (vous pouvez également protéger le BIOS par mot de passe). (Voir aussi "Restreindre l'accès aux lecteurs de disquettes et CD ROM" dans le chapitre *Stratégies générales*.)

Protection physique

- Il est difficile de recommander des protections physiques pour le matériel informatique. Vous devriez mettre en œuvre les pratiques de la section "Protection Physique", plus bas.
- Nous *recommandons* que les disques extractibles avec des systèmes de fichiers NTFS soient verrouillés de façon à ce que le personnel non habilité ne puisse les retirer. (Voir "Protection Physique " dans les Notes qui suivent.)

L'utilisation d'autres Systèmes d'Exploitation pour installer Windows NT

- Nous *suggérons* que vous n'utilisiez pas d'autres systèmes d'exploitation comme DOS ou Windows 95 pour installer Windows NT parce qu'ils peuvent créer des fichiers sur le système qui ne soient pas fait pour l'environnement Windows NT le plus sécurisé (bien que le risque soit faible). Assurez vous que tous les autres systèmes d'exploitation soient purgés avant d'installer Windows NT, ou reformatez les disques durs pendant l'installation. Si ce n'est pas possible, nous *recommandons* que vous enleviez tous les fichiers et répertoires des systèmes d'exploitation non-NT qui ne sont pas installés par Windows NT.

Boot d'un support alternatif

- Désactivez tout ce qui peut être utilisé pour booter d'autres systèmes d'exploitation. Voir "Démarrage d'autres systèmes d'exploitations" dans les Notes qui suivent. Malheureusement, vous avez peut être du matériel qui ne supporte pas ces protections, et s'il le peut, vous devriez évaluer les risques soigneusement. La facilité avec laquelle il est possible de booter sur une disquette fait courir d'énormes risques à la fois au Niveau 1 et 2.

Installation d'autres systèmes d'exploitation

- N’installez aucun autre système d’exploitation (comme DOS, Windows 95, ou Linux) sur un ordinateur Windows NT.[3] Voir “Démarrage d'autres systèmes d'exploitations” dans les notes qui suivent.
- N’installez pas plus d'un exemplaire de Windows NT sur un ordinateur à moins que cela ne soit operationellement nécessaire.[4] Certains administrateurs installent une seconde copie de secours de Windows NT Workstation qui n’a aucun utilisateur à part l' administrateur local avec un mot de passe convenablement sécurisé. Cette pratique est acceptable aux Niveaux 1 et 2, pourvu que vous preniez les précautions exposées dans la section “Copies Multiples de Windows NT sur un Ordinateur”, dans les notes qui suivent.

Le système de fichiers NTFS

- Nous *recommandons* que vous formatiez tous vos disques qui le peuvent en NTFS – et non pas FAT.[5] Le système de fichier FAT n’a pas d’ACLs et offre fondamentalement moins de sécurité pour les données. (Le bit “lecture seule” sur les fichiers FAT peut être enlevé par n’importe qui.) Vous pouvez utiliser des volumes FAT tant qu’ils ne contiennent pas le répertoire racine du système d’exploitation ou des fichiers ou dossiers qui n’auraient pas été autorisés en "Contrôle Total" pour Tout le Monde, si le système de fichier possédait des ACLs. Tant bien même, utilisez FAT seulement s’il y a une raison opérationnelle astreignante de le faire, et sur Windows NT il y en a rarement. Notez que Windows NT peut reformater des partitions pendant l’installation a partir de disquettes – il n’est pas nécessaire que vous formatiez en NTFS au préalable.

Enlever les sous-systèmes POSIX et OS/2

- Il y a peu d’information disponible sur la confiance que l’on peut porter aux sous-systèmes OS/2 et POSIX, bien qu’il n’y ait pas de raison de suspecter qu’ils posent un problème de sécurité majeure.[6] Nous *recommandons* que vous désactiviez ces sous systèmes à moins qu’ils ne soient nécessaires. Désactivez les en enlevant “Os2” et “Posix” de la chaîne “Optional” dans la base de registre:

```
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\
    Session Manager\Subsystems
```

---

[3] Il y'a certainement des cas ou des d'autres OS peuvent être installés et utilisés sans compromettre la sécurité de Windows NT, mais vous devriez soigneusement penser et évaluer les risques dans ces situations.

[4] Les systèmes de développement on souvent légitimement besoin d'avoir plusieurs copies de Windows NT installés, les développeurs nécessitent souvent des accès et privilèges que l'on ne donnerait pas à un utilisateur ordinaire. Ces systèmes devraient être isolés si possible.

[5] FAT fait référence au format de support Windows NT qui ne permet pas d'ACLs sur ses fichiers et dossiers, bien qu'il y'ait des cas ou un périphérique FAT entier puisse avoir une ACL.

[6] WOW (Windows on Win32) est le sous système Windows NT qui supporte les anciennes applications 16-bit Windows . Dans la relecture de ce document, Paul Ashton souligne qu'il y'a certains problèmes de sécurité avec WOW. Il serait prudent de le désactiver si vous ne l'utilisez pas (si vous n'utilisez que des applications récentes 32-bit). Cependant, comme pour POSIX et OS/2, il est difficile d'évaluer le degré de risque que WOW présente.

Ne pas faire d'installation par Copie

- Contrairement à la pratique recommandée, certains administrateurs installent Windows NT en copiant tout le répertoire racine système et quelques autres fichiers d'un ordinateur à l'autre. Ne le faites pas. Chaque installation de Windows NT reçoit un identifiant système unique parmi tous les identifiants du réseau, ce qui fait que l'identifiant de chaques groupes et comptes est unique lui aussi. Les "installations Copiées" n'ont pas cette unicité et cela peut fausser certaines protections de sécurité. (Voir [KBase] Q162001.) Notez qu'il y a des programmes de "clonage" qui corrigent ce problème.[7]

Notes

Démarrage d'autres systèmes d'exploitation

La plupart des ordinateurs, plus particulièrement ceux à base de processeurs Intel , populaires dans la communauté Windows NT, peuvent charger un système d'exploitation (comme DOS ou Windows 95) à partir de disquettes, même quand Windows NT est installé sur l'ordinateur. Ceci peut ce produire quand le BIOS de ces ordinateurs cherche les lecteurs de disquettes pour un support bootable avant le disque dur à partir duquel Windows NT boote. Vous devriez empêcher cela aux Niveaux 1 et 2 parce que les programmes peuvent être exécutés sur ces autres systèmes d'exploitation qui lisent et écrivent sur les partitions NTFS, en déjouant totalement la protection des ACLs.

La configuration firmware sur la plupart de ces ordinateurs (communément appelé le "BIOS" et habituellement activé par des touches spéciales pendant le démarrage) comporte des options soit pour empêcher de démarrer à partir de disquettes, soit de booter à partir de disquettes si aucun disque dur bootable n'est trouvé. Configurez une de ces options (de préférence la dernière) si votre ordinateur le permet.

De toute façon, cela n'empêche pas quelqu'un de remettre à zéro cette option. La plupart des ordinateurs ont aussi un mot de passe BIOS qui garde l'accès du programme BIOS et vous devriez définir un tel mot de passe. Du fait que pour deviner le mot de passe il faille l'entrer manuellement, ce mot de passe ne nécessite pas d'être aussi complexe que celui de Windows NT. Toutefois, vous ne devriez pas vous servir d'un mot de passe trop simple. Cependant, sur la plupart des ordinateurs, vous pouvez contourner le mot de passe en faisant certaines modifications sur les circuits internes de l'ordinateur.

Autrement, vous pouvez enlever le lecteur de disquette ou acheter des systèmes de verrouillage des lecteurs de disquette qui empêchent leur utilisation. Certains ordinateurs permettront peut être de booter a partir d'autres support extractibles, comme le CDROM, et les mêmes précautions s'appliquent. Notez que les techniques pour assigner une ACL au lecteur de disquettes (voir "Restreindre l'Access aux lecteurs de disquettes et CDROM " dans *Stratégies Générales*) n'empêchent pas de les utiliser comme périphérique de démarrage.

Certains ordinateurs peuvent être démarrés par des ordinateurs distants. A moins qu'ils aient une protection cryptographique, ils sont vulnérables aux menaces sur des réseaux non sécurisés. (Voir *Mise en Réseau*.)

Protection Physique

Il y a plusieurs raisons pour lesquelles vous pouvez avoir besoin de sécuriser physiquement l'ordinateur pour empêcher des utilisateurs non autorisés d'accéder a l'intérieur du bureau: le

[7] Voir http://www.ntinternals.com/ntsid.htm pour une liste exhaustive.

mot de passe BIOS peut souvent être détourné en accédant à la carte mère de l'ordinateur, du matériel extractible peut être enlevé pour des raisons de sécurité et être réinstallé, le disque dur peut être enlevé et remis dans d'autres systèmes où les données peuvent être lues ou modifiées, et bien qu' un peu moins probable, un intrus pourrait insérer du matériel nuisible dans le bureau.

Il y peu de choses que vous puissiez faire pour prévenir les abus du personnel, notamment avec des supports extractibles comme les lecteurs de disquettes ou les CDROM inscriptibles sauf à retirer le lecteur, le verrouiller physiquement, ou en mettant en place une ACL. (Voir " Périphériques & ACLs sur les Volumes Non-NTFS" dans *Stratégies Générales*). Les disques partagés extractibles, spécialement ceux qui sont formatés en NTFS, devraient être verrouillés physiquement, sinon ils pourraient été installés sur d'autres systèmes d'exploitation et verraient leur données lues ou modifiées, en contournant les contrôles d'ACL NTFS. Ce n'est généralement pas aussi important pour les supports formatés en FAT car il n'y a aucune attente de confidentialité concernant les données contenues sur ces disques. Ils ne présentent pas plus de risque que des disquettes excepté qu'ils contiennent plus de données. Toutefois, si vous protégez un périphérique FAT avec une ACL (voir "Restreindre l'Access aux lecteurs de disquettes et CD-Roms" dans *Stratégies Générales*), les utilisateurs peuvent penser que les données contenues sont confidentielles et le retrait deviendrait alors un problème plus envisageable.

Copies Multiples de Windows NT sur un Ordinateur

Vous devez prendre quelques précautions si vous installez plus d'un exemplaire de Windows NT sur un ordinateur. (Remarquons qu'une option de démarrage et son choix "Mode VGA" correspondent à un seul exemplaire.) Windows NT ouvre certains fichiers en mode exclusif quand il démarre pour empêcher les programmes non sécurisés d'y accéder, notamment les fichiers dans WINNT\System32\CONFIG qui contiennent le Registre. Ces fichiers peuvent avoir des ACLs qui autrement autoriseraient un tel accès, bien que ce guide recommande de les protéger plus étroitement. De tels fichiers sont exposés sur les exemplaires de Windows NT autres que celui qui est actif.

Il y' a des cas où les ACLs créées par un des exemplaires ne sont pas protégées correctement quand un autre exemplaire est actif. Par exemple, supposez que deux exemplaires de Windows NT reconnaissent un compte de domaine appelé "JJones." Le premier exemplaire de NT a un copie du groupe local appelé GroupeX qui contient Jjones, et une ACL qui refuse l'accès au GroupeX, et rejette JJones. Cet ACL ne refuse pas l'accès JJones quand le second exemplaire de Windows NT est activé car GroupeX apparaît comme un groupe "Inconnu" au deuxième exemplaire.

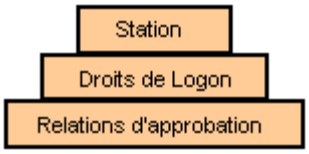
Toutefois, les utilisateurs et groupes "prédéfinis" suivants ont la même identité sur tous les systèmes Windows NT: Tout le monde, Interactive, Network, System, Administrateurs, Utilisateurs, Invites, Utilisateurs avec Pouvoirs, Réplicateurs, Opérateurs de Serveur, Opérateurs Imprimantes, Opérateurs de Sauvegarde, Opérateurs de Comptes, CREATEUR/PROPRIETAIRE , et Utilisateurs Autorisés. Les ACLs qui ne contiennent que ces identités sont toujours correctement appliquées et respectées par des versions co-résidentes de Windows NT.

4. Domaines & Restrictions d'Accès de base

L'aspect le plus fondamental dans la conception d'un réseau Windows NT est de déterminer quels comptes utilisateurs peuvent accéder à quels ordinateurs. Les restrictions de sécurité de Windows NT sur cet accès sont puissantes, fondamentales, et ne sont pas contournées par les autres stratégies d'accès NT. Cet aspect de la conception du réseau est donc par conséquent un des plus important, en partie parce qu'il est aussi un des plus difficile à modifier par la suite.

Par "accès" nous voulons dire connexion locale ou a distance. Une **connexion locale** désigne le fait qu'un utilisateur soit assis devant son ordinateur et se connecte pour établir une session. Une **connexion a distance** est invisible à l'utilisateur et se produit quand il accède pour la première fois aux ressources réseau à partir d'un autre ordinateur, où la deuxième connexion a lieu. Avant d'installer votre réseau Windows NT, vous devez concevoir une structure de domaine qui empêche de manière optimale les comptes utilisateurs d'accéder à des ordinateurs pour lesquels ils n'ont pas d'autorisation. Il y a trois aspects fondamentaux dans cette conception:

- La **structure** de base **du domaine** du réseau (appartenance au domaine et relations d'approbation), comprenant l'utilisation de comptes locaux "correspondants" pour aider à conserver une structure de domaine simple en l'adaptant a des situations spécifiques. Les domaines déterminent fortement et fondamentalement quel compte utilisateur a accès à quel ordinateur sur le réseau Windows NT. Les domaines isolent aussi le contrôle administratif du réseau. Les administrateurs d'un domaine n'ont pas de contrôles administratifs dans d'autres domaines sans l'action expresse de l'administrateur de l'autre domaine.



- Les droits de se **connecter localement** et **à distance** dans la stratégie des droits de chaque ordinateur déterminent qui peut se connecter à cet ordinateur. Parce que vous devez maintenir cela sur chaque ordinateur, il est important que vous développiez une stratégie spécifique (voir *Droits des Utilisateurs*).
- Les **restrictions de connexions sur les stations de travail** assignées a chaque compte déterminent les sites de connexion locaux. Chaque compte de domaine peut avoir une liste des ordinateurs à partir desquels l'utilisateur est autorisé à se connecter. Ce peut être mis en place de manière utile, bien qu'il ne concerne que les connexions locales et qu'il soit limité à 8 stations de travail. (Voir aussi *Comptes utilisateurs et Groupes.*)

Il ne peut y avoir de conseils spécifiques pour concevoir cette structure. Vous devez comprendre les principes des domaines et des comptes correspondant, et les appliquer à l'installation. Voir les Notes plus bas qui s'étendent sur ces trois sujets, ainsi que les Références Générales à la fin de ce chapitre.

Recommandations

Niveaux 1 & 2:

Concevez soigneusement votre stratégie globale du réseau sur ces trois principes déterminants de quels utilisateurs peuvent utiliser quels ordinateurs, comme dit dans les Notes qui suivent. Alors que le Niveau 1 implique un certain degré de prévision et de planification, le niveau 2 justifie une large analyse du site. Au Niveau 1, on se focalise sur le

fait de tenir les utilisateurs non authentifiés à l'écart des informations sensibles et des ressources centrales, comme des contrôleurs ou des serveurs. Au Niveau 2, tous les répertoires donnés du réseau devraient être la considération principale. Il est important de complètement développer cette conception *avant* que vous installiez votre réseau.

Examen Périodique:

Revoir la structure du domaine et l'utilisation des autres mécanismes pour bloquer les comptes primaires. L'audit devrait évaluer comment ces mécanismes renforcent ce qui suit:

- Aucun compte ne devrait avoir accès a un ordinateur, dont la stratégie de site l'empêche d'y avoir accès. (Niveau 1 et 2)
- Pour le niveau 2, vous devriez réévaluer les stratégies de comptes si en gros plus de 10% des comptes sur l'ensemble du réseau ont accès à des ordinateurs dont les propriétaires des comptes n'ont pas besoin pour leur mission opérationnelle.

Notes

Pour souligner l'importance de planifier les domaines et la structure de base de compte, nous présentons plusieurs longues descriptions de ces fonctions de base. Vous pouvez aussi consulter les Références Générales à la fin de ce guide.

Domaines, Approbations & portée des Comptes

Tous les réseaux Windows NT de taille appréciable sont mieux gérés quand ils sont sous divisés en domaines. Un domaine est un ensemble d'ordinateurs membres d'un ou deux types : les ordinateurs sur lesquels le produit appelé "Windows NT Workstation" est installé dans sa configuration de membre du domaine, et les ordinateurs sur lesquels le produit "Windows NT Server" a été installé dans sa configuration "serveur". Nous nous référons aux deux comme "stations de travail" même si le dernier peut travailler comme un serveur de groupes de travail. Une station de travail peut être membre d'un seul domaine, et reste généralement dans le même domaine. Les administrateurs contrôlent l'appartenance d'une station de travail à un domaine.

Chaque domaine possède un **contrôleur de domaine primaire** qui sert de contrôleur d'authentification des utilisateurs de son domaine et peut établir des relations d'approbation avec les contrôleurs d'autres domaines. Chacun d'entre eux peut avoir un ou plusieurs **contrôleurs de sauvegarde de domaine** qui se partagent la charge d'authentification du contrôleur principal, et l'un d'eux sera promu primaire si le principal est hors fonction. Tous les contrôleurs de domaine communiquent régulièrement entre eux pour assurer à chacun d'avoir une copie des bases de données essentielles d'authentification. Nous omettons largement de parler des contrôleurs de sauvegarde car ils n'ajoutent rien au niveau des considérations de sécurité pour structurer les domaines Windows NT.

Un contrôleur de domaine contient un jeu des **comptes du domaine**. Chacun de ces comptes de domaine peut être utilisé pour établir des sessions de connexions localement ou à distance sur chaque ordinateur du domaine (à moins qu'un contrôle l'en empêche). Chaque ordinateur dans un domaine, y compris le contrôleur de domaine peut aussi contenir des **comptes locaux**. Un compte local peut être utilisé pour établir des connexions localement ou à distance uniquement sur l'ordinateur dans lequel il est contenu.

Les administrateurs de deux domaines peuvent établir des relations d'approbation d'un domaine à l'autre. Si un domaine A approuve un domaine B, alors tous les comptes utilisateurs du domaine B peuvent être utilisés pour des connexions locales ou distantes sur

les ordinateurs de A. Bien que, les comptes du A ne peuvent être utilisés en B à moins que les administrateurs établissent un relation d'approbation séparée où B approuve A. La phrase "A approuve B" signifie que le contrôleurs de domaine de A permet (approuve) aux comptes de B de se connecter, que se soit localement ou a distance, à tous les ordinateurs de A (à moins qu'un contrôle secondaire ne l'en empêche)." Notez que si A approuve B, et B approuve C, il *n'est pas vrai* que A approuve C. Pour que cela se produise, il faut que les administrateurs de A et C paramètrent A comme approuvant C directement.

Par convention, la plupart des comptes sur l'environnement réseau du domaine sont des comptes de domaines. Les comptes locaux sont le plus fréquemment utilisés pour les ouvertures de session distantes pour des utilisateurs dont la portée de compte côté client n'est pas dans celle du serveur.

La manière dont vous sous-divisez votre réseau en domaines est un contrôle fondamental, et dans beaucoup de cas le critère le plus important pour déterminer quel utilisateur peut utiliser quel ordinateur, que ce soit par accès distant ou local. Votre but global est d'utiliser les structures des domaines pour contraindre les utilisateurs à n'utiliser que les ordinateurs pour lesquels ils ont reçu l'autorisation.

Il y a deux techniques importantes qui vous aident à garder une relation d'approbation sur le réseau simple et "efficace". La première utilise les comptes locaux correspondants. Supposez que vous ayez besoin de donner un accès à un utilisateur de A à un ordinateur (que ce soit une station de travail ou un contrôleur de domaine) dans le domaine D, mais D n'approuve pas A. Y' a-t-il besoin de configurer D pour approuver A pour servir ce seul utilisateur? Non. A la place établissez un compte local sur l'ordinateur dans D, en lui donnant le même nom et mot de passe que cet utilisateur. Notez que cela fonctionne seulement sur l'ordinateur qui contient le compte correspondant, D dans ce cas. (Voir "Mots de passe pour les Comptes Locaux Correspondants" dans *Mots de passes*.)

La deuxième technique empêche un compte d'accéder à un ordinateur alors que la structure de domaine l'aurait normalement autorisé, et implique de refuser de donner les droits de se connecter localement et/ou "accéder a cet ordinateur à partir du réseau " à partir du compte sur cet ordinateur. (Voir "Droits de connexion dans les environnement à plusieurs domaines " plus bas.) Il y a aussi les restrictions "se connecter à" sur les stations de travail dans chaque compte du domaine, mais ils gèrent seulement la connexion locale (primaire) et sont limitées à 8 station de travail. (Voir *Comptes utilisateurs et Groupes*.)

Comptes & Authentification Réseau[8]

L'identité de l'utilisateur, telle qu'elle est représentée dans son compte utilisateur, est la base de son accès aux capacités et services réseau de bases sur Windows NT . A quelques exceptions près, Windows NT ne prend en compte aucune demande pour les opérations basiques à moins que celles-ci ne soient faites par un compte utilisateur adéquat qui puisse être utilisé sur l'ordinateur exécutant la requête. (Un certain nombre de contrôles limitent l'ordinateur sur lequel un compte peut être utilisé.) Les utilisateurs ne sont jamais représentés par un compte à moins qu'ils n'en connaissent le mot de passe (à l'exception peut-être de certains cas "sûrs" contrôlés par le système).

[8] Cette section décrit les mécanismes d'authentification utilisés par les systèmes de partage réseau de Windows NT. Cependant, quelqu'un peut installer des services (comme FTP) qui n'utilisent pas ces mécanismes, des contrôles comme le Droit d'ouvrir une session à distance ne contraignent pas de tels services. L'on devrait évaluer la sécurité de tels services au cas par cas..

Les comptes locaux peuvent être conservés sur n'importe quel ordinateur NT et leur portée ne concerne que ce seul ordinateur. **Les comptes de domaine** sont stockés sur des contrôleurs de domaine (et leurs contrôleurs de sauvegarde respectifs), et leur portée inclue tous les ordinateurs qui sont membres de ce domaine (y compris les contrôleurs de domaines) ainsi que tous les ordinateurs de tous les domaines qui approuvent le domaine qui contient le compte.

Quand un utilisateur se connecte physiquement à un ordinateur NT, ils doit présenter un compte dans la portée de cet ordinateur ainsi que son mot de passe. Avant qu'ils se déconnectent, toutes leurs activités locales sont représentées par ce compte. Nous appelons cela une **connexion locale** (ou **connexion primaire**).

Quand un utilisateur connecté à distance essaie d'utiliser un service réseau , comme se connecter à un répertoire partage ou une imprimante, Windows NT approuve en utilisant un service administratif à distance, l'ordinateur distant établit une session **connexion à distance** qui dicte les demandes au serveur distant. Nous utilisons les termes de "client" et "serveur" pour décrire les ordinateurs locaux et distants. Bien que les détails varient selon le compte utilisé, dans tous les cas il s'agit d'un compte qui puisse être utilisé sur le serveur sur lequel l'utilisateur montre qu'il connaît le mot de passe.

Si le compte client de l'utilisateur est un compte de domaine dans la portée de l'ordinateur distant en vertu de la configuration du domaine, ce serveur utilise le même compte. Bien que le serveur essaie de trouver un compte du même nom. S'il est trouvé et que le mot de passe est différent, l'utilisateur doit entrer le mot de passe. Dans certains cas l'utilisateur peut plutôt fournir un compte arbitraire sur la portée du serveur ainsi son mot de passe. (Cette procédure varie selon les différents scénarios de connexion à distance.)

Une fois que l'utilisateur client établit une connexion à distance sur un serveur, toutes les demandes supplémentaires à ce serveur (comme se connecter à d'autres partages sur le serveur) sont associées au compte sur le serveur initial. Les sessions à distance sur les serveurs ne se terminent que lorsque l'utilisateur se déconnecte localement.

Chaque ordinateur Windows NT possède un compte prédéfini appelé **Invité** qui peut être désactivé mais ne peut être effacé. Si le compte Invité est actif et comporte un mot de passe vierge, la plupart des serveurs représentent un client distant en utilisant ce compte lorsqu'il ne peut fournir un nom et un mot de passe dans la portée de ce serveur. De ce fait, c'est une connexion distante non authentifiée et elle n'est pas conforme a la stratégie sécuritaire de la majeure partie des sites. Pratiquement tous les guides de sécurité Windows NT recommandent de désactiver tous les comptes Invités à moins d'avoir une stratégie acceptable pour leur utilisation.

Pour résumer, un utilisateur ne peut obtenir des services d'un ordinateur tant que l'ordinateur n'établit pas une session connexion associée à un compte actif; soit la session est une connexion locale pour un utilisateur directement connecté, soit une connexion distante à partir d'un ordinateur client distant. L'utilisateur doit d'une certaine manière démontrer qu'il connaît le nom d'un compte et son mot de passe contenu sur l'ordinateur serveur. Une exception notable est que dans de nombreux cas le compte Invité du serveur, s'il est activé, peut être utilisé pour établir une connexion distante, côté serveur sans que l'utilisateur ait à fournir de renseignements.

Dans de rares occasions, il est possible à un utilisateur d'obtenir les services d'un ordinateur Windows NT sans une connexion secondaire réussie. Ces mécanismes sont souvent appelés **connexions anonymes** et nous en parlons dans une section plus loin.

Modèles de Domaines

Plusieurs publications parlent de différents schémas de modèles de domaines pour les relations d'approbation. (Voir par exemple les références plus bas.) Nous ne les répéterons pas, mais nous mentionnons un modèle commun pour les petites et moyennes installations appelé modèle de Domaine de Ressource. Un seul domaine "maître" contient tous les comptes pour le site. Un jeu de domaines "ressources" approuve tout le domaine maître et ne définit pas de comptes particuliers. Les domaines ressources ne sont pas concernés par l'administration globale des sites, chaque domaine de ressource est la base pour définir des groupes administratifs. Le contrôle des comptes utilisateurs globaux et les groupes restent à la charge des administrateurs du domaine maître, tandis qu'au contraire les administrateurs de chaque domaine de ressource gardent peut être le contrôle exclusif des ressources du domaine.

Droits de connexion dans des environnements à plusieurs domaines

De nombreux sites utiliseront les groupes Utilisateurs et les groupes globaux Utilisateurs du Domaines pour contrôler leurs connexions locales et distantes. Ceci implique d'assigner des droits de "se connecter localement" et "accéder à cet ordinateur à partir du réseau" de manière appropriée, peut-être en combinant de manière différente ces groupes sur chaque ordinateur comme suit:

- Incluez le groupe Utilisateur du Domaine à partir du domaine natif de l'ordinateur dans le groupe local de l'utilisateur. (Par défaut il y est déjà.)
- Décidez si le groupe local Utilisateurs doit inclure des groupes d'Utilisateurs de Domaine d'autres domaines. (Par défaut ce n'est pas le cas.)

  Note: Cette décision devrait être appliquée de manière homogène à travers un domaine, et de préférence avec tous vos réseaux de domaines.
- Assignez le droit "se connecter localement " à la combinaison des groupes utilisateurs et Utilisateurs de Domaines de façon à être compatible avec votre stratégie sécuritaire sur l'ordinateur concerné. Procédez de façon identique avec le droit "accéder à cet ordinateur par le réseau", celui ci peut évidemment avoir différentes combinaisons des groupes cités précédemment.

Les exemples suivants montrent différentes combinaisons d'appartenance au groupe local Utilisateur, et les groupes assignés aux droits locaux et distants ("réseau"). Ceci est une stratégie ouverte sur une station de travail NT qui permet à tous les utilisateurs définis de tous les domaines visibles de se connecter localement et à distance:

Utilisateurs contient:	Utilisateurs de Domaine de *tous les domaines visibles.*
Se connecter localement:	Utilisateurs
Accès a distance:	Utilisateurs

Notez bien que, le seul fait d'assigner à un compte le Droit d'accéder à cet ordinateur à distance ne signifie pas qu'ils peut le faire à moins qu'il y ait un partage adéquat ou qu'un autre contrôle le permette.

Un exemple de deux stratégies équivalentes, qui permettent le partage à distance à partir de domaines choisis, mais pas les connexions locales:

Utilisateurs contient:	Utilisateurs de Domaine du *domaine natif seulement*
Connexions locales:	Utilisateurs
Connexions a distance:	Utilisateurs, Utilisateurs de Domaine des *domaines non natifs choisis*

Utilisateurs contient:	Utilisateurs de Domaine des *domaines natifs et non natifs choisis*
Connexions locales:	Utilisateurs de Domaine du *domaine natif*
Connexions a distance:	Utilisateurs

Ce qui suit est un exemple de stratégie ouverte sur un Serveur de Domaine ou un Contrôleur de domaine qui restreint étroitement les connexions locales (ce qui est recommandé pour ces systèmes) mais permet largement les partages :

Utilisateurs contient:	Utilisateurs de Domaine du *domaine natifs et tous ceux qui sont approuvés*
Se connecter localement:	*les administrateurs choisis (la configuration par défaut de Windows NT)*
Se connecter à distance:	Utilisateurs

Si vous désirez des contrôles plus affinés pour les connexions locales et à distance, ajoutez les utilisateurs choisis pour ces Droits. (Utilisez les groupes plutôt que les comptes quand c'est possible pour simplifier la maintenance.) Par exemple, la combinaison suivante (où "JJones" est le seul utilisateur régulier pour cet ordinateur) limite la connexion locale mais permet largement le partage de fichier:

Utilisateurs contient:	Utilisateurs de Domaine du *domaine natif & et tous ceux visibles*
Se connecter localement:	JJones, Utilisateurs avec pouvoirs du Domaine, & Administrateurs
Se connecter à partir du réseau:	Utilisateurs

Il est difficile de priver les connexions locales ou à distance pour les comptes choisis parce qu'ils sont généralement membres du groupe Utilisateurs. Vous devriez plutôt remplacer Utilisateurs avec les comptes autorisés dans la stratégie des Droits. L'accès local et/ou à distance des groupes que nous avons décrits peut être utile ici.

Il y a beaucoup de raisons liées à la sécurité pour restreindre les connexions locales et/ou à distance plus étroitement que le domaine le permet. Par exemple, il est courant dans les environnements à plusieurs domaines de permettre à un domaine A d'approuver un domaine B pour que les comptes du B puissent accéder à distance aux services réseaux des serveurs dans le domaine A. Bien que, cela implique que les comptes du domaine B puissent se connecter localement sur la machine dans A, ce qui n'avait peut être pas été prévu. Il est possible mais moins probable que la situation soit inversée, que l'approbation soit créée pour permettre les connexions locales mais pas à distance.

Chapitres liés:

Droits d'Utilisateurs

Comptes Utilisateurs et groupes

Structure Administrative

Références:

[Sutt96] Chapitre 6, *Planning Domains*. Planification des Domaines et "modèles de domaine."

[ConPln] Chapitre 1, *Administration des Domaines Windows NT Server*. Planification des Domaines et "modèles de domaine."

[KBase] Q102716 et Q122422 fournissent des descriptions techniques sur l'authentification, bien qu'ils soient de bas niveau.

5. Structure Administrative

Ce chapitre explique la configuration et l'utilisation des comptes administratifs et opérateurs. Il n'est recommandé aucune reconfiguration des comptes standards de Windows NT, mais nous offrons des recommandations sur la portée et les missions des comptes du personnel administratif. Notez qu'il y a différentes techniques alternatives qui sont aussi puissantes.

Recommandations

Le compte "Administrateur"

Chaque ordinateur Windows NT possède un compte Administrateur qui peut être renommé, mais pas effacé. (C'est un compte global sur les contrôleurs de domaines et un compte local autrement.) Vous définissez le mot de passe de ce compte pendant l'installation de Windows NT et il sert comme seul compte administrateur complet de base. Le compte Administrateur ne peut être verrouillé à cause de tentatives échouées, répétées de connexions (comme peuvent l'être les autres comptes) et bénéficie donc d'un mot de passe plus complexe.

Ce guide *recommande* que toute l'administration du système soit faite par d'autres comptes administratifs (en bas) et ce compte local Administrateur doit être utilisé comme compte de maintenance de dernier ressort.

Niveau 1:

Les techniques suivantes sont *recommandées*:

- Pour chaque domaine définir un mot de passe de 14 caractères composés de symboles clavier aléatoires imprimables, mélangeant minuscules et majuscules. Ecrivez le mot de passe et conservez le dans un endroit sûr où seul le personnel pleinement administrateur administratif peut accéder. Votre réseau est aussi sûr que cet endroit.
- Assignez ce mot de passe au compte de l'Administrateur local sur chaque ordinateur du domaine.
- Modifiez ces mots de passe si un Administrateur qui les connaît part de votre établissement, ou si vous suspectez les mots de passe d'avoir été compromis.

Ce guide ne recommande pas que ces mots de passe soient changés de façon régulière et systématique, bien qu'il n'empêche pas cette pratique.

Niveau 2:

Les mots de passe de cette complexité ne sont pas susceptibles d'être découverts par les méthodes connues d'attaque par "force brute" [9]. Bien, parce qu'il y a toujours quelques risques minimaux liés au stockage des mots de passe sur une ordinateur, au Niveau 2 il parait prudent de ne pas utiliser le même mot de passe sur les stations de travail des utilisateurs et pour les ordinateurs sensibles du réseau, comme les contrôleurs de domaine et les serveurs de données majeurs. Un "serveur majeur " est n'importe quel ordinateur qui contient une importante quantité de données sensibles de diverses sources. Cette technique est aussi une précaution utile contre les mots de passe administratifs oubliés. En ajout des procédures du Niveau 1:

[9] Remarquons que l'ancienne authentification LANMAN peut rendre ces longs mots de passe vulnérables sur le réseau. Voir "Mots de passe LANMAN" dans le chapitre *Mise en Réseau* pour désactiver ce format.

- Définissez et stockez un deuxième mot de passe de la même complexité. Assignez le au compte administrateur des ordinateurs sensibles du réseau: (1) contrôleurs de domaine (qui incluent leurs contrôleurs de sauvegarde parce que leur base de données comptes est répliquée automatiquement), (2) serveurs importants (voir la suite), et (3) chaque ordinateur qui sert de passerelle pour un intranet qui n'est donc pas totalement sécurisé.
- Facultativement, vous pouvez définir davantage de mots de passe administratifs de ce type au point que chaque ordinateur puisse posséder le sien. Cependant, tant que votre stratégie de site permette l'administration par des Administrateurs "Pleins Pouvoirs", leur mot de passe sont susceptibles d'être le véritable maillon faible.

Examen Régulier:

- Revoyez la sécurité de mots de passe écrits, sous clés, y compris les conditions dans lesquelles l'on a pu y accéder pour l'utilisation.
- Revoyez régulièrement si ces mots de passe doivent être modifiés suite à changement du personnel.

Administrateurs "Pleins Pouvoirs"

Chaque compte qui est membre du groupe prédéfini Administrateurs local possède virtuellement des pouvoirs illimités sur cet ordinateur et, s'il s'agit d'un contrôleur, sur le domaine complet. Nous appelons ces comptes des **administrateurs "Pleins Pouvoirs"**. Le compte administrateur est par défaut membre de ce groupe. Un but majeur est d'utiliser ces comptes le plus rarement possible, en se servant à la place de comptes avec moins de pouvoir pour les activités quotidienne.

Niveau 1:

Les techniques suivantes sont *recommandées*:

- Suivez la politique d'administration standard de Windows NT en utilisant les comptes administrateurs de domaine uniquement pour les taches d'administration totale. Assignez ces comptes aux groupes globaux Administrateurs de domaines. Sur chaque ordinateur du domaine, assurez vous que le groupe Administrateurs de domaine soit membre du groupes local administrateur, de la même manière que le compte local Administrateur (la configuration par défaut).
- Créez un tel compte administratif et distribuez son mot de passe aux quelques personnes en qui vous avez confiance pour l'administration totale. Voir "Comptes Administratifs Partagés " dans les Notes qui suivent. Appelez ce compte comme vous le voulez. Certains préfèrent des noms obscurs, voir "Renommer les Comptes Administrateur," plus bas.
- Si un des domaines approuve un second domaine, les Administrateurs de Domaine du second domaine peuvent être inclus dans tous les groupes Administrateurs locaux sur les ordinateurs du premier. Ceci permet aux administrateurs totaux du deuxième domaine de complètement administrer le premier, et cela reste sujet à la stratégie de votre site.

Niveau 2:

Sur les réseaux plus larges, ce guide *recommande* de séparer la totalité de l'administration des stations de travail de celles des systèmes sensibles (contrôleurs de domaine et serveurs sensibles).

- Définissez un groupe global "Administrateur de Station de Travail " sur le contrôleur de domaine et ajoutez le dans le groupe local Administrateurs sur toutes les stations de travail du domaine.

- Créez un compte “Administrateur de Station de travail” sur chaque domaine et ajoutez le dans le groupe Administrateur des stations de travail. Distribuez son mot de passe a ceux qui sont censés être les administrateurs des stations de travail, probablement un groupe plus réduit que les autres administrateurs.
- Ce guide recommande que les groupes Administrateurs de Domaines des autres domaines, s'ils sont présents, soient retirés du groupe local Administrateur des stations. Les comptes Administrateurs peuvent être utilisés à travers les domaines s'il l'on peut les considérer comme suffisamment sécurisés.

Note: Alors que vous pouvez considérer les Administrateurs de Stations ("Workstation") comme moins fiables en terme de confiance que les Administrateurs de Domaines, tous les Administrateurs "Pleins Pouvoirs" doivent être dignes de confiance et protéger activement leur compte.

Examen Régulier:

- Au niveau 1, un réseau où plus de 2% de ces utilisateurs sont administrateurs devrait considérer une réévaluation de l’assignation d’administration totale. (1% pour le Niveau 2)
- Pour les réseaux moyens (100-1000 ordinateurs), l’usage de comptes administratifs sur des périodes plus longues qu'une semaine devrait entraîner une réévaluation de la structure administrative du réseau.

Opérateurs de Domaine & Utilisateurs avec Pouvoirs

Les opérateurs de contrôleurs de Domaine (Serveur, Imprimante, Compte et Sauvegarde) et Utilisateurs avec Pouvoirs ainsi que les Opérateurs de sauvegarde sur les stations de travail (les comptes “opérateur”) sont conçus pour la plupart des tâches administratives quotidiennes. Ces rôles devraient être utilisés pour le but recherché.

Niveaux 1 & 2:

Les rôles d’opérateurs devraient être utilisés pour toutes les activités quotidiennes afin d' éliminer le besoin des comptes d’administrateurs "Pleins Pouvoirs". Il est acceptable pour un compte de détenir plus d’un de ces rôles si la personne est digne de confiance pour l'utilisation de ces responsabilités combinées.

- Les comptes opérateurs ne devraient pas être partagés entre les utilisateurs. Nous *recommandons* l'utilisation d'un compte personnel, conçu pour une utilisation exclusive durant une certaine tache, et inclut dans le groupe opérateur approprié. Si cette personne doit effectuer des tâches non opérationnelles, donnez lui un compte “personnel” séparé, qui n’est pas membre des groupes opérateurs.
- Les Opérateurs de Sauvegarde ont les droits de Sauvegarde et Restauration qui contournent les ACLs. N’importe quel programme malintentionné qu’ils peuvent exécuter peut complètement renverser le système de sécurité et, si c’est un contrôleur de domaine, la sécurité même du domaine (voir *Spoofing*). Les comptes assignés aux Opérateurs de Sauvegarde ne doivent **jamais** être utilisés pour des tâches autres que celles de sauvegarde et de restauration.
- Par précaution, enlever les deux Droits de sauvegarde et de restauration de fichiers et répertoires du groupes Opérateurs de Sauvegarde sur les ordinateurs qui n’en ont pas

besoin. Par exemple, là où les programmes de sauvegarde du réseau n'ont pas besoin d'appartenance à ces groupes.

- Les opérateurs de contrôleur de domaine sont des groupes locaux et ne peuvent être utilisés ailleurs que sur le contrôleur de domaine, bien que certaines opérations puissent être faites à distance quand un opérateur est connecté sur un autre ordinateur. En particulier au Niveau 2, nous *recommandons* que vous limitiez les ordinateurs à partir desquels les opérateurs peuvent se connecter. Le danger premier est qu'ils puissent être "spoofés" quand ils se connectent à des ordinateurs qui ne sont pas strictement contrôlés. (Voir *Spoofing*.)

Ce guide *recommande* la technique suivante qui peut être adaptée pour des sites plus importants :

- **Utilisateurs avec Pouvoirs du Domaine**: Créez un groupe "Utilisateurs avec Pouvoirs du Domaine" et incluez le dans le groupe local Utilisateurs avec Pouvoirs sur chaque stations de travail, excepté pour les systèmes sensibles. Placez les comptes du domaine dans les Utilisateurs avec Pouvoirs du Domaine qui sont approuvés pour exécuter des tâches correspondantes à leur statut pour toutes les stations de travail dans le domaine. Autorisez l'utilisation à travers les domaines si c'est approprié en incluant les groupes Utilisateurs avec Pouvoirs du Domaine des autres domaines dans le groupe local Utilisateurs avec Pouvoirs de la station.

  Les comptes qui sont membres à la fois du groupe Opérateurs de Compte et Opérateurs de Serveur peuvent être placés dans Utilisateurs avec Pouvoirs du Domaine et devrait alors être autorisés à se connecter à ces stations de travail.

Examen Régulier:

- Assurez vous que les utilisateurs soient membres uniquement des groupes qui correspondent aux taches dont ils ont opérationellement besoin.
- Déterminez le niveau auquel les opérateurs puissent utiliser leurs comptes pour des tâches autres que les fonctions opérationnelles. Cela devrait être minimisé.
- Assurez vous que les comptes Opérateurs de Sauvegarde n'exécutent pas des commandes système ou des opérations autres que la sauvegarde et la restauration.

Pratiques Administratives

- Les administrateurs devraient suivre les pratiques suivantes. Au Niveau 1, ceci devrait être observé par les administrateurs "Pleins Pouvoirs", et au Niveau 2 par tous les administrateurs (excepté peut être les Opérateurs d'Imprimante, dont les capacités sont minimales; ceci inclut les Utilisateurs avec Pouvoirs).
  - Les administrateurs devrait se connecter uniquement lorsque c'est nécessaire.
  - Les administrateurs devraient porter une grande attention à minimiser l'usage de ce compte. S'ils se retrouvent quotidiennement amenés à exécuter des tâches qui ne nécessitent pas toutes les capacités administratives, ils devrait trouver un moyen de réaliser cette tache avec un compte moins puissant (moins il le sera mieux cela sera).
  - Les administrateurs ne devrait jamais exécuter des travaux personnels quotidiens, (lire les E-mail, surfer sur le Web, faire des rapports hebdomadaires) quand ils sont connectés à leur compte administrateur total. (L'une des techniques dans *Applications & Répertoires personnels* vous aide à empêcher les administrateurs d'exécuter ces programmes par inadvertance.)

- Les administrateurs devraient toujours mettre un mot de passe dans leurs économiseurs d'écrans. (Voir “Verrouillage d’Economiseur d’Ecran ” dans *Stratégies Générales*.)
- Tous les utilisateurs, particulièrement les administrateurs, devraient prendre connaissance des différentes attaques de “spoofing”. (Voir *Spoofing*.)
- Pour une sécurité maximale et cependant pratique, les administrateurs devraient travailler sur des ordinateurs dédiés à l’administration, en gérant le réseau à distance. Généralement, des ordinateurs aussi sécurisés que possible. Ils devraient contenir les utilitaires administratifs, et pas contenir d'applications générales (traitements de texte, navigateurs et autres). L'accès à ces ordinateurs devrait être strictement contrôlé par le fait de (1) donner le droit de se connecter localement uniquement aux administrateurs autorisés, et (2), si possible, ne donner à personne le Droit de se connecter à distance et ne pas permettre de partages de fichiers. Pour étendre la pratique, les administrateurs qui utilisent ces ordinateurs dédiés ne devraient pas être autorisés à se connecter localement à d’autres ordinateurs par leur Stratégies de Droits.

Notes

Comptes Administratifs Partagés

Il est commun et il semble juste que les utilisateurs administratifs totaux ne partagent pas leurs comptes, et que chacun devrait avoir son propre compte administratif. Cependant, ce guide ne requiert pas cette pratique au Niveau 1 et les petits sites de Niveau 2 (bien que l'on ne soit pas contre) pour les raisons suivantes:

- Un administrateur total n’est pas protégé contre un autre qui serait malintentionné. Tous les objets créés par les administrateurs totaux appartiennent au groupe Administrateurs local, des techniques spéciales sont nécessaires pour qu'un administrateurs puisse protéger ses travaux.
- Dans un réseau convenablement configuré, les comptes administrateurs totaux sont rarement utilisés.
- Partager un seul compte signifie que tous les administrateurs sont d’accord sur le mot de passe, et cette pratique empêche un tel compte d’être un maillon faible en ayant un mot de passe mal choisit.

La différence majeure entre les comptes administratifs personnels et partagés est que l’audit ainsi que les autres systèmes d'enregistrement peuvent distinguer les actions respectives des comptes. (Notez que les administrateurs totaux peuvent modifier de tels enregistrements de telle façon que les comptes personnels ne soient pas une protection contre un administrateur malintentionné et déterminé.) Cependant, ce guide apprécie la valeur des comptes administratifs personnels, spécialement sur les sites plus importants, et les laisse en tant qu'alternative potentiellement intéressante. Notez que les comptes administratifs totaux autres que les comptes Administrateurs prédéfinis sont complètement sujets au verrouillage.

L’utilitaire PASSPROP

L’utilitaire appelé “PASSPROP” du Ressource Kit Windows NT 4.0 a une fonction de verrouillage qui soumet le compte Administrateur local à la stratégie de verrouillage en vigueur mais ne verrouille que les connexions distantes (pas locales) des Administrateurs. Bien que ce soit une bonne fonction, les chances pour qu’un intrus trouve les mots de passes aléatoires que nous recommandons est infinitésimale et PASSPROP n’est pas strictement nécessaire.

Renommer le Compte Administrateur

Certains sites renomment les comptes administratifs avec un nom obscure pour rendre plus difficile la détermination des connexions administratives, bien que certains qualifient cette méthode de “sécurité par l'obscurité”. Le but de cette pratique est d’augmenter le nombre de combinaisons d'utilisateurs et de mots de passe possibles, bien qu'il soit toujours mieux d’augmenter la complexité du mot de passe. Windows NT considère le mot de passe comme une donnée privée alors que les noms utilisateurs sont considérés comme des informations publiques sur un réseau Windows NT. Les comptes administratifs renommés ne restent pas “secrets” très longtemps. (Voir “Utilisateurs & Noms de Partages disponibles aux utilisateurs non authentifiés” pour noter que Windows NT permet aux connexions non authentifiées d'accéder à certaines données, relativement bénignes, comme les noms des utilisateurs et les partages.) La taille du mot de passe Windows NT peut convenir aux plus exigeants en terme de longueur donc il n'y a pas réellement besoin d'obscurcir un nom de compte parce que le mot de passe serait trop court.

L'un des avantages d'obscurcir un compte administrateur se présente lorsqu'un administrateur enlève son mot de passe par mégarde. En contrepartie, la pratique consistant a renommer le compte administrateur n’offre pas suffisamment de protection pour justifier sa présence dans nos conseils. Les administrateurs qui choisissent de les renommer sont avertis de ne pas réduire la complexité de leurs mots de passe. Utilisez toujours une taille de mot passe conforme à vos besoins de sécurité comme si vous n’aviez pas renommé le compte.

Chapitres liés :

Spoofing, sur les dangers pour les opérateurs d'exécuter des programmes dangereux.

Comptes Utilisateurs & Groupes (commentaires généraux sur la complexité du mot de passe)

Références:

[Sutt96] “ Administrateurs totaux” dans le Chapitre 7, *Gérer les Groupes et les comptes*, p. 185.

[Sutt96] “Opérateurs” et “Utilisateurs avec Pouvoirs” dans le Chapitre 7, *Gérer les Groupes et les comptes*, p. 188, 190.

[ConPln] Chapitre 2, *Travailler avec des comptes Utilisateurs et Groupes*.

6. Stratégie Générale

Ce chapitre contient divers mais importants conseils pour l'administration générale du système. Bien qu'ils puissent paraître parfois obscurs et détaillés, ils présentent les décisions importantes que vous devez prendre tôt dans la mise en place de votre sécurité. Remarquez que les conseils de ce chapitre et ceux de *Spoofing* sont liés avec ceux de la partie Conseils & Notes. Les conseils présentés correspondent aux paragraphes de notes précédents.

Conseils & Notes

Périphériques & ACLs sur les Volumes Non-NTFS

Certain objets dans la hiérarchie interne de Windows NT permettent l'accès direct en écriture et en lecture sur des périphériques de stockage, comme les disques durs, contournant ainsi les ACLs incluses dans le système NTFS. Ces objets sont accessibles seulement aux administrateurs globaux et ne nécessitent aucun ajout de protection.

Tous les volumes logiques (tout ce qui a un lettre disque, comme "D:") sont liés par un objet dans la hiérarchie, l'ACL de ce lien commande l'accès à ce volume en sus des contrôles supplémentaires éventuels, comme les ACLs de NTFS. Configurer cette ACL sur le lien (l'ancre) d'un volume NTFS parce que l'ACL dans ce format protège ses propre objets. Toutefois, certains sites désireront peut être appliquer une ACL sur cette ancre pour empêcher l'accès au volume dans son ensemble. Par ailleurs, certains sites voudront peut-être empêcher l'accès à certaines unités physiques, comme les disques extractibles, en utilisant l'ACL de l'ancre. Voir [KBase] Q150101. Il n'y a aucun outil dans Windows NT qui permette de configurer ou de voir l'ACL d'une ancre, bien qu'il y ait des outils fournis par des sociétés tierces qui le fassent.[10]

Restreindre l'Accès aux lecteurs de disquettes et au CD-ROM

La clé de la Base de Registre:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT
   \CurrentVersion\Winlogon
```

peut avoir les valeurs REG_DWORD appelées "AllocateFloppies" et "AllocateCD-Roms." Si leur valeur est à 1, l'accès aux lecteurs de disquettes et aux CD-ROMs, respectivement, est inaccessible à l'utilisateur actuellement connecté à cet ordinateur. (Notez que les lecteurs de disquette et de CD-ROM sont parmi les périphériques qui n'ont pas d'ACL intégrée.) Ces entrées ne protègent pas les autres périphériques comme les lecteurs de bandes ou les périphériques extractibles. (Voir aussi la partie " Périphériques & ACLs sur les Volumes Non-NTFS," plus bas.)

[10] Par exemple, "WinObj" à partir de http://www.ntinternals.com.

Conseils

Niveaux 1 & 2:

- Protégez les lecteurs de disquettes et CD-Roms (comme nous venons de le décrire) en configurant AllocateFloppies et AllocateCD-Roms à 1. Vous pouvez protéger les lecteurs de CD-ROM sur les ordinateurs prévus pour le partage réseau. Marquez physiquement de tels lecteurs comme “NON PRIVES” pour prévenir les utilisateurs d'éventuels dangers.
- Nous *recommandons* que vous cherchiez des applications tierces qui appliquent des ACLs sur les périphériques tels que les lecteurs de disquette et configurez-les en fonction de la stratégie de votre site.[11]

Accès à Distance Non Authentifiés (“Anonyme”) à la Base de Registres

Windows NT permet que l’on édite sa Base de Registres à partir d’un ordinateur distant sous une authentification secondaire standard, et sous le plein contrôle des ACLs de la base de registres. Le Service Pack 3 (SP3) de Windows NT 4.0 a corrigé un problème où des utilisateurs distants non authentifiés pouvaient obtenir l'accès à la base de registres d'un ordinateur sous le groupe "Tout le monde". (Le pseudo-groupe "Tout le monde" se réfère ici uniquement aux comptes authentifiés.) Ceci est aussi appelé accès "anonyme". L'accès anonyme peut être restauré en modifiant deux valeurs dans la clé :

```
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\
   LanmanServer\Parameters
```

D’abord, définissez une valeur REG_DWORD appelée **RestrictNullSessionAccess** et donnez lui la valeur 1. Ensuite, ajoutez la chaîne “WINREG” à la valeur multichaîne (multistring) appelée **NullSessionPipes**. Le fait de définir la valeur de RestrictNullSessionAccess à 1 informe Windows NT qu’il autorise l’accès anonyme aux éléments listés dans NullSessionPipes et NullSessionShares. Par défaut, RestrictNullSessionAccess n’est pas défini.

Les Utilisateurs non authentifiés sont inclus dans le groupe tout le monde, mais pas dans les autres groupes. En particulier, le groupe **Utilisateurs Authentifiés** ajouté dans le SP3 exclut l'accès anonyme. Si vous devez autoriser l'accès anonyme à la base de registres, vous pouvez donc contrôler un tel accès en utilisant Utilisateurs Authentifiés dans les endroits où vous auriez autrement utilisé Tout le Monde.

Certaines applications dépendent d’un accès non authentifié (notamment, certaines applications de sauvegarde) et ne marcheront peut-être pas correctement si l'accès anonyme est enlevé de la Base de Registres.

Voir aussi “Restreindre l'accès à la base de registres à distance,” qui suit.

Se référer a [KBase] xQ143138, Q126645, et Q143474.

Conseils

Niveau 1:

[11] Il existe un freeware appelé “FLock” par Konstantin Sobolev (sob@cmp.phys.msu.su) de l'Université d'Etat de Moscou qui permet d'appliquer des ACLs aux lecteurs de disquettes et CDROM. Il y'a aussi un produit commercial appelé “SmartSecurity” d' Insight Software Solutions, Inc. sur http://smartcode.com/iss qui applique des ACLs à une grande variété de périphériques Windows NT. Faites attention aux interactions entre “AllocateFloppies” et “AllocateCDRoms,” et de tels applications tierces. Testez les protections rigoureusement.

- Evitez d'autoriser l'accès anonyme si cela est faisable. Si vous devez l'utiliser pour vous adapter à certaines applications, minimisez ses effets en utilisant Utilisateurs Authentifiés à la place de Tout le Monde dans les portions de la base de registres où l'accès anonyme n'est pas autorisé.

Niveau 2:

- N'autorisez pas la connexion anonyme sur les portions de la Base de Registres excepté pour les zones ou l'accès anonyme ne représente pas une menace.

Restreindre l'accès à la Base de Registres à distance

Si la clé suivante existe dans la Base de Registres:

```
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\
   SecurePipeServers\WINREG
```

Alors seulement les utilisateurs listés dans son ACL, ou ceux qui appartiennent aux groupes listés dans son ACL, peuvent avoir accès à la base de registres à distance.

> **Note**: Les permissions assignées à ces entrées ACL n'ont aucun effet. Ainsi, en ajoutant a un groupe le droit de lecture ne lui permettra pas d'accéder à la base de Registre en lecture uniquement. Les permissions spécifiques pour accéder à des clés de la base de registre a distance sont déterminées uniquement par les ACL des clés auxquelles les utilisateurs essaient d'accéder.

Quoi qu'il en soit, les clés de la base de registres sont chacune listées comme une valeur REG_MULTI_SZ dans la clé:

```
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\
   SecurePipeServers\Winreg\AllowedPaths\Machine
```

Définissez des clés de registre dans `HKEY_LOCAL_MACHINE` qui soient différentes des ACL de WINREG. Ces clés et toute leur arborescence sont exemptes du contrôle WINREG, et leur accès uniquement gouverné par les ACLs des clés. (Ces noms de clés sont en accord avec `HKEY_LOCAL_MACHINE.`)

L'accès anonyme à distance autorisé par NullSessionPipes se fait seulement sous le groupe Tout le Monde, et en tant que tel restreint par l'ACL sur la clé WINREG. Ceci étant, à moins que le groupe Tout le Monde n'apparaisse dans les ACLs de WINREG, ou à moins que la clé à laquelle on accède soit dans AllowedPaths de WINREG, l'accès anonyme n'est pas autorisé, même si les NullSessionPipes vous y autorisaient.

Se référer à [KBase] Q153183, Q155363, et Q157474.

Conseils

Niveaux 1 & 2:

- Créez la clé WINREG et ajoutez les groupes suivants à l'ACL (avec n'importe quelle permission):
  Utilisateurs authentifiés
- Au Niveau 2, nous *recommandons* que vous enleviez l'entrée Utilisateurs Authentifiés et ajoutiez les utilisateurs ou groupes uniquement lorsque cela est opérationellement nécessaire (comme les Administrateurs ou Utilisateurs avec Pouvoirs du Domaine, si mis en place). La capacité de lire une base de registres à distance peut offrir des renseignements pour une attaque, et il semble peu sage de permettre cette capacité sans une raison opérationnelle importante.

- Initialement, assurez vous que la clé “Machine” n’a pas de valeur. Vous pourrez ajouter des valeurs où c’est nécessaire et après vous être assuré que ces clés dans ces chemins ont des ACL appropriées.

Activer les Editeurs de Registre

Si la clé dans la base de registre:

```
HKEY_CURRENT_USER\Software\Microsoft\Windows
   \CurrentVersion\Policies\System
```

a une valeur appelée “DisableRegistryTools” avec une valeur REG_DWORD de 1, les outils standard d'édition de la base de registre ne fonctionneront pas. Vous pouvez les démarrer, mais ils se ferment avec un petit message de sécurité. Vous pouvez configurer ceci pour ne pas autoriser l’usage de ces outils sur un ordinateur, ou pour l'intégrer dans un schéma de stratégie de fichiers Système. Il est possible de faire la même chose en mettant l’ACL sur les fichiers exécutables pour que les éditeurs de base de registres afin d'autoriser seulement certains utilisateurs ou groupes la permission (“X”) à exécuter le programme, et refuser l'accès lecture (“R”) aux autres utilisateurs (ce qui les empêche de copier le programme et d'exécuter la copie).

Quoiqu’il en soit, cette protection n'empêchera peut-être pas aux utilisateurs d'accéder à la base de registres en utilisant d’autres outils disponibles, y compris ceux que les programmeurs peuvent aisément créer. Cette protection n’est pas une barrière même pour un utilisateur malveillant peu sophistiqué. Les seules protection valables pour la base de registres sont ses ACLs.

Conseils

Niveaux 1 & 2:

- Bien que le fait de désactiver les éditeurs de la base de registres offre peu de protection, désactivez les sur les ordinateurs où il n’y en a pas besoin. Les fichiers de Stratégie permettent une technique utile, où vous pouvez les activer pour des utilisateurs choisis, en général les administrateurs (voir Fichiers de Stratégie Système). Autrement, vous pouvez mettre une ACL sur les programmes d'édition de la base de registres (REGEDT32.EXE et REGEDIT.EXE) comme décrit précédemment.

ProtectionMode

Invisible pour la plupart des utilisateurs, le système d’exploitation Windows NT possède une hiérarchie interne qui contient un certain nombre d’objets accessibles aux programmes de l’utilisateur. Beaucoup de programmes créent des objets dans cette hiérarchie comme si cela faisait partie de leurs activités normales, et ces objet peuvent avoir des ACLs. Quoiqu’il en soit, par défaut beaucoup de ces objets ont une configuration vague ou pas d’ACL. Ils sont vaguement référencés comme “Objets de Base” (Base Objects). Cette enquête ne peut trouver aucune définition publique claire de ces objets, bien que la rumeur dise qu’ils incluent des segments de mémoire partagée et des objets de synchronisation inter-processus (décrits dans l'API Win32), les ports de communication, et les affectations aux lettres des lecteurs.[12]

[12] Ce doit être les contrôle utilisé par l'utilitaire C2CONFIG pour restreindre la redéfinition utilisateur des "lettres de lecteurs et imprimantes".

En modifiant la valeur REG_DWORD appelée “ProtectionMode” à 1 dans la clé de la base de Registres:

```
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control
   \SessionManager
```

l'on est censé placer une sorte de protection ACL pour ces objets qui limiterait l'accès à leurs créateurs et administrateurs. Bien que la suffisance de ces protections ait été approuvée dans l'évaluation originale C2 de Windows NT, les descriptions publiques de la signification de ces protections sont vagues.[13] Le consensus actuel est que cette valeur devrait être mise sur les installations Windows NT soucieuses de leur sécurité.

L'activation du ProtectionMode peut faire que les utilisateurs se voient privés d'opérations qui ne sont peut être pas significatives en terme de menace de sécurité. Si ces problèmes se développent, désactivez le ProtectionMode. Malheureusement, il n’y aucune manière générale d’ajouter des informations d’audit sur ces objets, alors l’utilisation de la technique d’audit (comme décrite dans “Installer & Tester de Nouvelles Applications ” dans *Système de Fichier et Paramètre d'ACL de la Base de Registres*) n’est pas applicable. Voir “Sécurité stricte pour les objets partagés ” dans [RKitW].

Conseils

Niveau 2:

- Ce guide *recommande* que vous activiez le ProtectionMode (décrit précédemment) à moins qu’il n’impose des contraintes opérationnelles inacceptables. Soyez **avertis que** le ProtectionMode peut perturber l'activité normale du système et ses effets peuvent être obscures. (Si la protection et les effets du ProtectionMode étaient mieux compris, nous les recommanderions certainement aussi au Niveau 1.)

Visualisation non Authentifiée du journal des événements

Par défaut, les invités et les utilisateurs non authentifiés peuvent lire les journaux d'événement Système et Application (mais pas le journal Sécurité). Vous pouvez empêcher cela en créant une valeur appelée “RestrictGuestAccess” avec un valeur REG_DWORD de 1 dans le clés de la base de registres:

```
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services
   \EventLog\Application
```

```
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services
   \EventLog\System
```

Appliquez cette protection sous l'hypothèse que les intrus puissent glaner des informations utiles à partir de ces enregistrements. Il ne devrait y avoir aucun impact défavorable sur la globalité des opérations du système. (Référence: “Secure Event Log Viewing” dans [Micr97].)

Conseils

Niveaux 1 & 2:

- Implémentez la protection ci-dessus mentionnée.

[13] Nous ne faisons qu'un commentaire purement formel concernant le fait qu'un composant potentiellement important de la sécurité de Windows NT apparaît comme étant non documenté.

Installation de Pilote d'Imprimantes

Vous pouvez restreindre la capacité d'ajouter des pilotes d'imprimantes aux administrateurs, Opérateurs d'Impression, et Utilisateurs avec Pouvoirs en créant une valeur appelée "AddPrinterDrivers" avec une valeur REG_DWORD de 1 dans la base de registres:

```
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control
   \Print\Providers\LanMan Print Services\Servers
```

Des pilotes d'impression peuvent détourner des données utilisateurs. (Voir "Sécuriser l'installation des Pilotes d'impression" dans [Micr97].)

Conseils

Niveaux 1 & 2:

- Implémentez la protection précédente.

Verrouillage de l'écran de veille

Le verrouillage automatique d'un ordinateur non utilisé est une protection de sécurité importante. (le "verrouillage" automatique produit le même effet que de verrouiller manuellement l'ordinateur depuis la Fenêtre Sécurité.) Plusieurs des économiseurs d'écrans fournis avec Windows NT ont cette fonction. Malheureusement, il n'y a pas de manière sûre, automatisée d'obliger les utilisateurs à les utiliser. Bien que vous puissiez utiliser des fichiers de Stratégie pour enlever le panneau des économiseurs d'écran du Contrôle de l'affichage, les utilisateurs peuvent en utiliser d'autres, en employant par exemple des outils disponibles pour modifier les entrées de la base de registres qui contiennent le nom de l'économiseur d'écran et ses paramètres.

Conseils

Niveaux 1 & 2:

- Comme nous en avons discuté précédemment, mettez en place une pratique de site qui contraigne les utilisateurs à activer le verrouillage de l'économiseur d'écran à chaque fois. Il n'y a pas de manière sûre, automatisée d'imposer ceci et vous devez en dernier lieu compter sur la coopération des utilisateurs. *Recommandé* au Niveau 1 et *prescrit* au Niveau 2.
- Ces conseils suggèrent un temps de 20 minutes pour verrouiller au Niveau 1, et 5 minutes au Niveau 2, bien que cela soit considérablement dépendant du site.

Protection des "Mots de passe cryptés" & SYSKEY

Windows NT ne conserve pas de copies des mots de passe utilisateurs, quoiqu'il en soit, il conserve une valeur cryptée ("hash") générée à partir du mot de passe (souvent appelé l' "OWF"). Vous pouvez considérer un mot de passe "hashed" comme un cryptage du mot de passe que personne ne peut décrire. Bien qu'une personne qui connaisse le mot de passe crypté d'un autre compte ne peut pas s'en servir directement pour se connecter, il y a des attaques relativement efficaces disponibles pour le détenteur de ce dernier. Le principal lieu de stockage de Windows NT pour les mots de passe cryptés se situe dans la base de registres, ce qui les protège de la vision publique. Cependant, ces mots de passe peuvent aussi apparaître dans d'autres endroits.

La commande SYSKEY permet au site d'augmenter la protection des mots de passes stockés localement. Par défaut, Windows NT stocke une version cryptée des mots de passe utilisateurs dans le Registre SAM auquel seuls les administrateurs globaux ont accès.

Quoiqu'il en soit, l'option /s de la commande RDISK et certains programmes de sauvegarde peuvent sauvegarder des copies des mots de passe cryptés avec moins de protection. Bien que la version cryptée ne puisse être utilisée pour se connecter directement, elle peut l'être par des programmes malintentionnés (mais sophistiqués) pour la connexion réseau, et peut être utilisée pour les attaques brutales de mots de passes. Ceci peut constituer un risque de sécurité significatif.

La commande SYSKEY vous permet de configurer le système pour que le mot de passe crypté de l'utilisateur soit à nouveau crypté avec un algorithme de 128-bits pour une protection supplémentaire. Hormis un défaut éventuel dans l'algorithme, il est réputé être absolument indestructible. Vous pouvez utiliser SYSKEY dans l'un de ces trois modes :

1. **Auto Boot**: Le système génère une clé de cryptage interne brouillée et la conserve sur le système. Ceci permet les démarrages automatiques sans intervention de l'utilisateur. Quoi qu'il en soit, si votre SAM sans protection SYSKEY est vulnérable, alors votre clé de cryptage l'est aussi. Ce mode est pratique mais sa sécurité est plus réduite.
2. **Floppy Boot**: Le système génère une clé complexe, aléatoire et la conserve sur une disquette que vous devez insérer pour lancer le système. La clé n'est pas stockée sur le système. Ce mode est plus sûre, mais si vous perdez la disquette (ou si un intrus la copie), vous serez en danger.
3. **Password Boot**: Vous, en tant qu'administrateur, choisissez un mot de passe qui est utilisé pour la base de la clé de cryptage, et qui est nécessité pour lancer le système. Encore, si vous oubliez le mot de passe ou s'il est découvert, vous serez en difficulté.

(La description de l'utilisation de SYSKEY est incluse et nous renvoyons le lecteur a [KBase] Q143475 pour plus de détails. L'option (3) utilise un mot de passe choisi par un administrateur. La taille du mot de passe détermine la puissance du cryptage face aux attaques brutales. Un mot de passe[14] aléatoire, de 14 caractère alphanumériques produit une clé dont la taille est d'à peu près 82-bits ce qui devrait être plus qu'adéquat pour tous les sites même les plus sécurisés. (En comparaison, le cryptage DES 56-bits est toujours puissant. Bien qu'il ait été cassé par force brute, cela a nécessité les ressources combinées de milliers d'ordinateurs sur Internet. Le cryptage 82-bits est a peu près 16 million de fois plus complexe que le 56-bits.) Le risque, évidemment, est qu'un tel mot de passe doit être écrit et consulté à chaque fois qu'il est entré– au moins un moment. Pour cela, le fait de protéger son image écrite revient au même que de protéger la disquette utilisée dans l'option (2).

Notez que le fait de connaître la clé de cryptage SYSKEY, le mot de passe administrateur ou bien de copier la disquette, ne permet pas à l'intrus de découvrir vos mots de passe décryptés. Ils doivent aussi casser les autres protections que vous appliquez grâce aux conseils suivants. En assumant que vous les appliquiez correctement, ils ont besoin d'avoir l'accès administratif global au système, et s'ils l'obtiennent, la sécurité est compromise dans tous les cas. Quoiqu'il en soit, l'utilisation de SYSKEY rend moins importante l'implémentation de ces autres protections.

[14] Consistant en des chiffres, et des caractères alphabétique majuscules et minuscules.

Conseils

Niveaux 1 & 2:

- Comme l'on vient de le décrire, protégez les répertoires WINNT\CONFIG et WINNT\REPAIR comme spécifié dans *Système de Fichier et Paramètres d'ACL de la Base de Registre*.
- Restreignez les médias suivants aux seuls administrateurs globaux et aux Opérateurs de Sauvegarde:
  - Les disques de réparation de secours créés avec l'option "/**s**" de la commande RDISK,
  - fichiers faits par les programmes variés qui sauvegardent la partie compte utilisateur de la base de registres (communément appelée la "SAM") en fichiers,
  - les cartouches de sauvegarde qui ont des copies de la base de registres, les copies de ses fichiers actifs ou les copies manuelles de ces fichiers, ou les copies des fichiers dans WINNT\CONFIG.
- Au Niveau 1, nous *recommandons* l'utilisation de n'importe lequel de ces trois modes de SYSKEY, en n'utilisant pas l'option (1) sur les contrôleurs principaux et secondaires, ou les serveurs sensibles. Effectivement, utilisez le mode SYSKEY (1) uniquement sur les stations de travail. Au Niveau 2, nous *prescrivons* l'utilisation des modes SYSKEY (2) ou (3).

La fonction de Notification du Mot de passe

Les administrateurs globaux peuvent installer des DLL que Windows NT active à chaque fois qu'un mot de passe est modifié, amenant le nouveau mot de passe à la DLL. Certaines DLL de ce type s'en servent pour forcer les restrictions mot de passe et d'autres l'utilisent pour synchroniser des éléments non-Windows NT avec le mot de passe Windows NT. La clé de la base de registre:

```
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa
```

peut avoir une valeur REG_MULTI_SZ appelée "Notification Packages" dont la valeur est une liste de noms de DLL (moins le suffixe ".DLL") qui réside dans le répertoire SYSTEM32. Il est essentiel que l'entrée de la base de registre nomme uniquement des DLL sûres qui existent dans SYSTEM32 et qui sont en lecture seule pour les personnes autres que les administrateurs globaux. Voir aussi [KBase] Q151082 et Q161990.

Conseils

Niveaux 1 & 2:

- Comme décrit précédemment, assurez-vous que Notification Packages est vide à moins que les DLL qu'il nomme soient installées et utilisées sur le système, et protégées avec une ACL appropriée.[15] Notez que de tels DLL sont assez spécialisées et ne sont pas nécessaires sur la plupart des installations Windows NT.

[15] Microsoft a fournit Windows NT 4.0 avec cette entrée de Registre positionnée sur "FPNWCLNT" mais sans la DLL correspondante. Cela signifie que quiconque peut créer un fichier dans SYSTEM32 peut installer une DLL malveillante en l'appelant simplement "FPNWCLNT.DLL". Les Services Packs ont résolu ce problème.

Utilisateurs & Noms de Partage disponibles aux utilisateurs non authentifiés

Windows NT permet à l'utilisateur qui, en vertu des relations d'approbation, n'a aucun accès à certains domaines de voir les noms de comptes des utilisateurs, ainsi que les partages réseau et imprimantes sur les ordinateurs de ces domaine. Pour prévenir cette vision anonyme des noms, on peut ajouter une valeur appelée "RestrictAnonymous" avec une valeur REG_DWORD de 1 à la clé:

```
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa
```

(Ce contrôle a été implémenté dans le SP3.) Quoiqu'il en soit, cette restriction empêche certaines fenêtres de lister de tels noms ou cela pourrait être utile pour à la fois les administrateurs et les utilisateurs normaux et légitimes. En outre, avant que les utilisateurs Windows NT puissent voir les noms de domaines auxquels ils n'ont pas accès, ils doivent se connecter et donc être authentifiés par NT. Pour cela, même si ils n'ont pas accès à certains domaines, ils sont pour le moins authentifiés dans au moins un domaine ou une station de travail. Par ailleurs, même si les interfaces communes ne listent plus de tels noms, les utilisateurs peuvent aisément écrire des programmes qui cherchent ces noms même si la restriction ci-dessus est en place. Le fait d'autoriser que ces noms soient visibles est un risque modeste. Pour ces raisons, le Guide ne prescrit pas l'emploi de cette méthode.

Cacher la dernière session utilisateur

Par défaut, Windows NT montre le nom du compte précèdent dans la fenêtre de connexion. Vous pouvez empêcher ceci en créant une valeur appelée "DontDisplayLastUserName" avec une valeur REG_SZ de "1" dans la clé de la base de registres:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\
    Current Version\Winlogon
```

Dans la plupart des cas c'est plutôt une protection inconséquente. Windows NT et de nombreuses communautés d'utilisateurs ne considèrent pas les noms d'utilisateurs comme un secret. Ils sont souvent des abréviations du nom de l'utilisateur et utilisés pour l'E-mail. La philosophie générale de Windows NT est de ne pas les garder secrets sur le réseau. L'accès à un compte utilisateur doit être gardé par son mot de passe, qui au contraire est un secret solide. Les ordinateurs dans des endroits "accessibles au public " devraient mettre en pratique cette fonction comme un principe général, mais ne comptez pas sur le masquage du dernier utilisateur pour apporter une amélioration significative de sécurité.

Conseils

Niveaux 1 & 2:

- Nous *recommandons* de configurer ce paramètre pour les ordinateurs déjà accessibles à des personnes qui n'ont pas de connexions sur le réseau.

Extinction du Système

Si la clé de la base de registres:

```
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\
    CurrentVersion\Winlogon
```

a une valeur appelée "ShutdownWithoutLogon" avec une valeur REG_SZ de "1," alors un bouton "Arrêt" apparaît à la fenêtre de connexion qui permet à quiconque d'éteindre le système sans y être connecté. Ce guide ne traite pas l'arrêt du système (un "dénie de service") en tant que problème de sécurité bien que cela puisse être un problème opérationnel important. Nous n'avons vu aucun exemple où l'arrêt du système puisse être utilisé pour

compromettre le système de sécurité sauf en tant que "dénie de service". Notez que ShutdownWithoutLogon est plus large que donner à Tout le Monde le droit “d'arrêter le système” parce que les Droits s’appliquent uniquement à un utilisateur valide qui s’est connecté, tandis que ShutdownWithoutLogon laisse les utilisateurs non authentifiés arrêter le système.

Gardez en tête que la plupart des stations de travail ont un interrupteur accessible. Un utilisateur déterminé à éteindre l’ordinateur peut très bien utiliser cet interrupteur s’il n’a pas d’autre solution, et il est possible que les données d'audit puissent être perdues dans ce cas, ce qui est un problème de sécurité. Donc, vous devriez bloquer l'accès à l’interrupteur de courant (la plupart des stations de travail ont une serrure pour cela). Mais il y aussi le cordon d’alimentation, les fusibles et ainsi de suite.

Conseils

Niveaux 1 & 2:

- Tandis qu’utiliser la clé de la base de registres pour empêcher d'éteindre les ordinateurs partagés est généralement une opération technique intéressante, le problème de sécurité le plus important est le fait de couper le courant de l’ordinateur, ceci peut entraîner la perte des données auditées. Si l’audit est un facteur important dans la stratégie de votre site, prenez toutes les protections que vous pourrez.

Hot-Fixes

Microsoft tient une liste de problèmes de sécurité fixés récemment sur:

http://www.microsoft.com/security

et une liste plus détaillée de “hot-fixes” post-SP3 sur:

ftp://ftp.microsoft.com/bussys/winnt/winnt-public/fixes/usa/NT40/hotfixes-postSP3

Microsoft a promptement diffusé des hot-fixes lorsque des défauts de sécurité ont été découverts sur Windows NT.

Conseils

Niveaux 1 & 2:

Téléchargez et appliquez les hot-fixes suivantes:

- Des hot-fixes sont disponibles pour quelques attaques en "dénie de service" qui peuvent arrêter ou ralentir le protocole TCP/IP. Voir [KBase] Q179129, Q165005, et Q154174.
- Un bug “GetAdmin” sous Windows NT permettait aux utilisateurs de devenir membre du groupe local d’Administrateurs et donc d’être tout puissants. Voir [KBase] Q165005.

Examen Régulier:

- Vérifier régulièrement les derniers hot-fixes et appliquez les lorsque c'est nécessaire.

L’outil C2CONFIG

Le Resource Kit [RKitS] de Windows NT contient un outil appelé C2CONFIG qui est censé vous dire si votre système est bien configuré comme “C2.” Malheureusement, le classement C2 n’est pas un critère opérationnel. Par exemple, bien que C2 nécessite un mécanisme d’audit sécurité, il ne cherche pas à forcer les administrateurs à l’activer. Personne ne peut dire qu’un système dont l’audit est désactive n'est “pas C2” – c’est simplement un système C2 dont les administrateurs ont choisit de ne pas auditer. C2 est une norme de produit qui

assure à l’acheteur qu’un système d’exploitation inclut certaines fonctions de sécurité et qu’il a été implanté d'une manière digne de confiance. Il n’indique pas que le système est “sécurisé” bien qu’il augmente notre confiance dans la sécurité inhérente au système. Malheureusement, le sens des évaluations C2 et DoD est terriblement mal compris dans la littérature actuelle.

L’outil C2CONFIG peut indiquer de manière utile quand vous avez activé les fonctions qui n'ont pas été évaluées pendant l'examen C2, et inspecte quelques paramètres de sécurité significatifs. Quoiqu’il en soit, vous ne devriez pas prendre de risque en vous disant que parce que vous avez passé l’outil C2CONFIG sur votre système qu'il suffisamment “sécurisé” pour votre situation, ou que si vous avez échoué à certains tests, que votre système ne l'est pas. Ce guide montre tous les aspects significatifs de sécurité de l’outil C2CONFIG.

7. Système de fichier et paramètres d' ACL

Windows NT initialise les ACLs à la racine du système de fichiers NTFS (principalement le répertoire WINNT) pour maximiser la compatibilité avec les applications Windows ce qui représente un risque modeste de sécurité. Bien que ces configuration d'ACL soient déjà sécurisées, il reste une marge considérable pour les affiner. Les ACL de la base de Registres la protègent raisonnablement par défaut. Quoiqu'il en soit, pour des raisons de compatibilité certaines de ces clés offrent plus de permissions que ce que la prudence imposerait. Les modifications plus bas réduisent à la fois les permissions NTFS et les ACL de la base de registres et s'appliquent aux Niveaux 1 et 2. La seule différence est que pour le Niveau 1 le critère de confiance pour inclure des utilisateurs dans le groupe Installateurs d'Applications est plus bas que dans le Niveau 2.

Après l'installation, le groupe "Tout le Monde" (que nous appelons le "Public" dans cette section parce qu'il peut aussi s'appliquer à d'autres groupes plus larges comme "Utilisateurs") possède un accès "écriture" sur certaines parties de la base de registres et sur l'arborescence du répertoire WINNT. Bien que ce ne soit pas un facteur flagrant de manque de sécurité, ces conseils mettent ces parties sous un contrôle administratif modeste au Niveau 1, et les réservent à une fonction administrative approuvée au Niveau 2.

Notre stratégie générale est de tout enlever à part l'accès à la lecture Publique (RX) des éléments dans des arborescences devant être restreint, et de donner toutes les permissions enlevées à un nouveau groupe local "Installateurs d'Applications". Ce groupe a donc toutes les capacités de Public après une installation NT standard. Nous utilisons le terme "installateur" parce que toutes les exigences pour créer de nouveaux éléments dans ces arbres viennent à l'installation de nouvelles applications ou matériels, ou à leur maintenance.

Au Niveau 1, Les Installateurs d'Applications peuvent inclure des utilisateurs normaux qui installent des applications qui ont besoin d'un accès écriture bénin sur WINNT et la base de registres. Alors qu'il est acceptable de placer tous les utilisateurs dans ce groupe, la pratique correcte est de ne pas le faire à moins que les applications des utilisateurs demandent un tel accès. Au Niveau 2, les Installateurs d'Application deviennent un groupe administratif, digne de confiance, bien qu'avec moins de capacités que les Administrateurs globaux.

A tous les niveaux, nous autorisons aussi les Installateurs d'Applications à ajouter les nouvelles applications aux répertoires officiels des applications. Ces sont des répertoires qui sont destinés à contenir des programmes sûrs, et approuvés. Voir "Répertoires d'Applications " dans *Applications & Répertoires Personnels*. Au Niveau 2, la surveillance administrative aide à garantir que toutes les applications résident bien dans ces répertoires.(On pourrait créer deux groupes: un pour WINNT et le second pour les répertoires d'applications, bien que nous ne revenions pas sur cette option.)

Les Installateurs d'Applications ne gagnent pas le contrôle complet aux répertoires d'applications, et aux arborescences de la base de registres et de WINNT. Typiquement, ils ont un accès "Ajout & Lecture" sur les répertoires, ce qui les laisse ajouter de nouveaux objets, mais au mieux un accès de Lecture sur les objets préexistants. Ils ont bien sûre le contrôle total sur les objets qu'ils créent. La différence entre les Niveaux 1 et 2 est le niveau de confiance placé dans les Installateurs Applications.

Les configurations recommandées réduisent aussi un certain nombre d'autres éléments dans WINNT et la base de registres pour les deux niveaux.

Note: Le résultat inévitable dans la restriction de ces ACLs est que certaines applications peuvent faillir lors de l'installation ou ne pas fonctionner correctement, et vous devez résoudre ces conflits au cas par cas. (Voir "Installer & Tester de Nouvelles Applications" dans *Système de Fichier & ACL du Registre*.) Vous allez aussi peut-être rencontrer d'autres problèmes opérationnels qui constitueront des compromis à envisager pour la sécurité. Quoiqu'il en soit, en tant que partie de cette étude, nous avons testé de nombreuses applications avec ces paramètres en obtenant relativement peu de conflit.

Conseils

Niveau 1:

- Nous vous *recommandons* de créer un groupe local "Installateurs d'Application " sur chaque ordinateur ainsi qu'un groupe "Installateur d'application du Domaine" dans chaque domaine. Remplissez ces groupes avec des comptes en lesquels vous avez confiance pour installer les logiciels. (Il n'est pas nécessaire d'inclure les administrateurs globaux dans Installateurs d'Applications parce qu'ils se voient donner l'accès total à tous les objets du système.)

  Note: Le groupe Installateurs d'Applications n'est pas strictement nécessaire, spécialement sur les petites installations. Vous pouvez à la place compter sur les administrateurs pour installer les logiciels. Si vous choisissez de faire ainsi, ne tenez pas compte des Installateurs d'Applications au niveau de la configuration ACL plus bas.

- Configurer les permissions sur le système de fichiers Windows NT comme défini dans les sections suivantes "Paramètres d'ACL pour le système de fichier," et sur la base de registres comme défini dans la section "Paramètres d'ACL de la Base de Registres"

Niveau 2:

En complément des procédures au Niveau 1:

- Assurez-vous qu'un minimum de personnel en qui vous ayez confiance soit dans le groupe Installateurs d'Applications. Globalement, il devrait y avoir autant de membres dans Installateurs d'Applications que dans le groupe d'administrateurs globaux.
- N'incluez pas des comptes à utilisation régulière dans Installateurs d'Applications. A la place, créez des comptes à utiliser uniquement lors de l'installation et incluez seulement ceux-ci dans Installateurs d'Applications. Vous pouvez inclure les comptes Opérateur de Serveur dans Installateurs d'Applications.

Examen Régulier:

- Assurez-vous que les protections prescrites sur la base de registres et WINNT ne soient pas abaissées sans raisons.
- Assurez-vous que l'appartenance au groupe Installateurs d'Applications est proportionnée par rapport à ce qui est dit plus haut dans le guide.
- Nous *recommandons* que vous cherchiez des outils pour vérifier l'intégrité de ces ACLs, comme le programme *Checker* développé avec ce contrat.[16] Autrement, revoyez les périodiquement.

[16] Allez sur le site Trusted Systems Services Web pour voir la disponibilité de Checker (http://www.TrustedSystems.com).

Notes

Paramètres d'ACL pour le système de fichier

Le système de fichier Windows NT contient plusieurs fichiers de sécurité sensibles, la plupart sont à la racine du répertoire système (usuellement mais pas nécessairement appelé “WINNT,” le nom que nous utilisons). Bien que raisonnablement protégé par défaut, pour des raisons de compatibilité de nombreux fichiers et répertoires sont laissés dans un état d'accès trop peu prudent pour les sites les plus sécurisés. Les modifications plus bas s’appliquent à la fois aux Niveaux 1 et 2. La seule différence est qu’au Niveau 1 le critère de confiance pour inclure les utilisateurs dans le groupe Installateurs d’Applications est plus bas qu’au Niveau 2. La table qui suit liste les ACLs recommandées pour les fichiers et répertoires standards de Windows NT:

- La première ligne de chaque groupe ci-dessous est le répertoire, et le reste est constitué par les fichiers (ou lorsque c’est noté les sous-répertoires) dans le répertoire.
- Les abréviations suivantes, utilisées dans la table, représentent les groupes locaux suivants:

  Public = Tout le monde
  Installeurs = Installateurs d’Applications
  SrvOps = Opérateurs de Serveur
  PwrUsers = Utilisateurs avec Pouvoirs

  En tant que stratégie de site, vous pouvez décider d'utiliser des groupes plus restrictifs tels que le groupe Utilisateurs Authentifiés, en tant que groupe Public.
- Les noms de permissions (comme “Lire” et “Ajouter & Lire”) sont ceux utilisés par l’ ACL de Windows.
- L'astérisque(*) après un jeu de permissions sur le répertoire indique que, si possible, les permissions sur le répertoire ne devrait pas être propagées sur des répertoires nouvellement créés. Bien que cela puisse se produire sur Windows NT, il n’y a pas d’interface Windows NT pour contrôler si cela se produit. Bien que cela ne soit pas nécessaire, c’est une pratique recommandée, vous aurez besoin d'outils de sociétés tierces[17] dans ce but.
- Toutes les ACLs suivantes sont censées inclure les entrées suivantes, qui sont standard sous WINNT:

  ACEs (Access Control Entries : Entrées de Contrôle d'accès) Communes à toutes les ACLs sous WINNT

CREATEUR/PROPRIETAIRE Administrateurs SYSTEM	Contrôle Total

- La notation “(aucun)”dans les tables signifie qu’il n'y a aucune ACE à l'exception des ACEs Communes
- Pour les répertoires listés, modifiez seulement l’ACL du répertoire (et pas ses sous répertoires) à moins que cela soit indiqué. Certains de ces fichiers et répertoires n’apparaissent pas à la fois dans les produits Windows NT Server et Workstation. Notez encore que la racine du système peut s’appeler autrement que “WINNT.”

[17] Super CACLS (http://www.TrustedSystems.com) est un produit commercial qui peut faire cela. Bien qu'il puisse en y avoir d'autre, aucun n'est fournit avec Windows NT ou le Ressource kit.

- Nous supposons que vous ayez installé Windows NT sur le volume C:. Si ce n'est pas le cas, faites les ajustements nécessaires dans le texte qui suit.
- Pour Windows NT Workstation, ignorez les Opérateurs de Serveur et d'imprimantes. Pour Windows NT Server, ignorez les Utilisateurs avec Pouvoirs.
- Ces paramètres modifient les permissions par défaut de Windows NT pour des Opérateurs variés, Utilisateurs avec Pouvoirs, ou d'autres groupes préexistants. Notre idée générale est que les Opérateurs de Serveurs possèdent un large accès aux répertoires et fichiers sensibles. Ils peuvent utiliser ces capacités pour avoir un accès administratif total grâce à des techniques de spoofing variées. Certains sites voudront peut-être tempérer cette stratégie.

	Recommandations	Install NT Std	Commentaires
C:	Installeurs: Modifier Public: Lire SrvOps: Modifier PwrUsers: Add*	Public: Modifier SrvOps: Modifier	Note : ACE qui ne se propagent pas
Fichiers	Installeurs: Modifier Public: Lire SrvOps: Modifier	Public: Lire SrvOps: Modifier	
IO.SYS MSDOS.SYS	Installeurs: Modifier Public: Lire SrvOps: Modifier	Public: Modifier	compatibilité 16-bit seulement. Supprimer si possible.
BOOT.INI, NTDETECT.COM NTLDR	*(none)*	Public: Lire	
AUTOEXEC.BAT, CONFIG.SYS	Installeurs: Modifier Public: Lire SrvOps: Modifier	Public: Modifier	Compatibilité 16-bit seulement. Supprimer si possible.
C:\TEMP	Public: (RWXD)*(NotSpec)	Public: Full	Note : ACE qui ne se propagent pas Voir note [7].
C:\WINNT	Installeurs: Modifier Public: Lire SrvOps: Modifier	Public: Modifier SrvOps: Modifier	Voir note [16] & [19].
Fichiers	Public: Lire SrvOps: Modifier	Public: Lire SrvOps: Modifier	
win.ini	Installeurs: Modifier Public: Lire SrvOps: Modifier	Public: Full	Compatibilité 16-bit seulement
control.ini	Installeurs: Modifier Public: Lire SrvOps: Modifier	N/A	
netlogon.chg	*(none)*	N/A	Fichier du contrôleur de domaine verrouillés par l'OS. Crée après l'installation.
\WINNT\config	Installeurs: Modifier Public: Lire SrvOps: Modifier	Public: Modifier SrvOps: Modifier	Tous les éléments de l'arborescence.
Fichiers	"	Public: Lire SrvOps: Modifier	
\WINNT\cursors **\WINNT\fonts**	Installeurs: Modifier Public: Add&Rd SrvOps: Modifier PwrUsers: Modifier	Public: Modifier SrvOps: Modifier	Tous les éléments de l'arborescence. Voir note [4].
Fichiers	"	Public: Lire SrvOps: Modifier	
\WINNT\help	Installeurs: Modifier Public: Lire SrvOps: Modifier PwrUsers: Modifier	Public: Modifier SrvOps: Modifier	Tous les éléments de l'arborescence, à l'exception de ceux présentés plus loin. Seuls *.HLP and *.CNT existent à l'installation.
Fichiers	"	Public: Lire SrvOps: Modifier	Voir note [2].
*.GID *.FTG *.FTS	Public: Modifier	"	Voir note [1]. Ces fichiers ne sont pas présents à l'installation.
\WINNT\inf	Installeurs: Modifier Public: Lire SrvOps: ??	Public: Modifier SrvOps: Modifier	Tous les éléments de l'arborescence. Seuls *.ADM, *.INI, & *.PNF installés.
Fichiers	"	Public: Lire SrvOps: Modifier	Voir note [3].
*.ADM	Public: Lire	"	Voir note [17].
*.PNF	Installeurs: Modifier		

	Public: Lire SrvOps: Modifier	Public: Modifier	

\WINNT\media	Installeurs: Modifier Public: Lire SrvOps: Modifier PwrUsers: Modifier	Public: Modifier SrvOps: Modifier	Tous les éléments de l'arborescence. Voir note [18]. Seuls *.RMI, *.MID, & *.WAV présent à l'install.
Fichiers	"	Public: Lire SrvOps: Modifier	
*.RMI	Public: Modifier	N/A	Voir note [18].
\WINNT\profiles	Installeurs: Add&Lire Public: (RWX)*(NotSpec)	Public: Modifier	Voir note [5].
Dir: *(nom utilisateur)*	*(idem que NT default)*	*User*: Full	
Dir: All Users Dir: Default	Installeurs: Modifier Public: Lire	Public: Lire	
\WINNT\repair	*(none)*	Public: Lire SrvOps: Full PwrUsers: Modifier	Tous les éléments de l'arborescence. Voir note [6]. Seuls les fichiers de ruche et deux fichiers *.NT sont présents à l'install.
Fichiers	*(none)*	N/A	Probablement gérés dynamiquement par NT.
\WINNT\system	Installeurs: Modifier Public: Lire SrvOps: Modifier	Public: Modifier SrvOps: Modifier	Tous les éléments de l'arborescence. Voir note [20]. Principalement *.DLL et *.DRV à l'installation.
Fichiers	"	Public: Lire SrvOps: Modifier	
\WINNT\System32	Installeurs: Modifier Public: Lire SrvOps: Modifier BckOps: Modifier	Public: Modifier SrvOps: Modifier	Idem que WINNT sauf pour les Opérateurs de Sauvegarde. Voir note [8] & [19]. Voir note [9].
Fichiers	Public: Lire SrvOps: Modifier	Public: Lire SrvOps: Modifier	
$winnt$.inf	Installeurs: Modifier Public: Lire SrvOps: Modifier	N/A	Voir note [10].
AUTOEXEC.NT CONFIG.NT	Installeurs: Modifier Public: Lire SrvOps: Modifier	Public: Modifier SrvOps: Modifier	Initialiser l'environnement DOS Voir note [10].
cmos.ram midimap.cfg	Public: Modifier	Public: Modifier SrvOps: Modifier	
localmon.dll decpsmon.* hpmon.*	Installeurs: Modifier Public: Lire SrvOps: Modifier PrintOps: Modifier PwrUsers: Modifier	Installeurs: Modifier Public: Lire SrvOps: Full PrintOps: Full PwrUsers: Modifier	
\WINNT\System32\config	Public: List	Public: Lire SrvOps: Modifier	Tous les éléments de l'arborescence. Voir note [6].
Fichiers	*(rien)*	Public: Lire SrvOps: Modifier	
default, software, system, userdiff	*(rien)*	N/A	
*.EVT	*(rien)*	*(rien)*	
\WINNT\System32\DHCP	Public: Lire SrvOps: Modifier	Public: Lire SrvOps: Full	Tous les éléments de l'arborescence. Voir note [21]. Vide à l'install.
Fichiers	"	Public: Lire SrvOps: Modifier	
\WINNT\System32\drivers (including **\etc** subdir)	Public: Lire	Public: Lire SrvOps: Full	Tous les éléments de l'arborescence. Voir note [11].
Fichiers	"	Public: Lire SrvOps: Modifier	
\WINNT\ System32\LLS	Installeurs: Modifier Public: Lire SrvOps: Modifier	Public: Modifier SrvOps: Modifier	Tous les éléments de l'arborescence. "License Logging Service."

Fichiers	“	“	

\WINNT\ System32\OS2 (incl **\DLL** subdir)	Public: Lire SrvOps: Modifier	Public: Modifier SrvOps: Modifier	Tous les éléments de l'arborescence. Voir note [12].
Fichiers	"	Public: Lire SrvOps: Modifier	
\WINNT\ System32\RAS	Public: Lire SrvOps: Modifier	Public: Modifier SrvOps: Full PwrUsers: Modifier	Tous les éléments de l'arborescence. Voir notes [13] and [22].
Fichiers	"	Public: Lire SrvOps: Modifier	
\WINNT\ System32\Repl	Public: Lire SrvOps: Full	Public: Lire SrvOps: Full	Tous les éléments de l'arborescence. Voir note [14].
Fichiers	"	*(none in std delivery)*	
\WINNT\ System32\Repl **\ import**, **export** … and "scripts" subdirs	Public: Lire SrvOps: Full Replicator: Modifier	Public: Lire SrvOps: Modifier Replicator: Modifier	
Fichiers	"	*(aucun en standard)*	
\WINNT\ System32\spool	Installeurs: Modifier Public: Lire SrvOps: Full PrintOps: Modifier PwrUsers: Modifier	Public: Lire SrvOps: Full PrintOps: Full PwrUsers: Modifier	Voir note [26].
Fichiers	"	Public: Lire SrvOps: Modifier	
\drivers **\drivers\w32x86\2** **\prtprocs** **\prtprocs\w32x86** **\ drivers\w32x86**	Installeurs: Modifier Public: Lire SrvOps: Full PrintOps: Modifier PwrUsers: Modifier	Public: Lire SrvOps: Full PrintOps: Full PwrUsers: Modifier	
Fichiers	"	Public: Lire SrvOps: Full PrintOps: Full PwrUsers: Modifier	
Fichiers dans ***drivers*****w32x86**\	"	Public: Lire SrvOps: Modifier	
\printers **\tmp**	Installeurs: Modifier Public: (RWX)(NotSec) SrvOps: Full PrintOps: Modifier PwrUsers: (RWXD)(WXD)	Public: Lire SrvOps: Full PrintOps: Full	Voir note [27].
Fichiers	"	Public: Lire SrvOps: Full PrintOps: Full	
\WINNT\ System32\viewers	Public: Lire SrvOps: Modifier	Public: Modifier SrvOps: Modifier	Tous les éléments de l'arborescence. Voir note [15].
Fichiers	"	Public: Lire SrvOps: Modifier	
\WINNT\ System32\wins	Public: Lire SrvOps: Modifier	Public: Modifier SrvOps: Modifier	Tous les éléments de l'arborescence. Voir note [23].
Fichiers	"	Public: Lire SrvOps: Modifier	
C: \ …*.EXE	Public: X	N/A	Voir note [24].
C: \ … ***.BAT** ***.COM** ***.CMD** ***.DLL**	Public: Lire	N/A	Voir note [24].
C:\ …*.INI sauf boot.ini	N/A	N/A	
\WINNT\system32 4 commandes BSD r*	*(rien)*	N/A	Voir note [25].

[1] Les fichiers History comme .GID doivent être accessibles à l'écriture publique pour être utilisés par plus d'un utilisateur. Il y a peu de risque à faire cela.

[2] Les fichiers d'aide peuvent contenir un code exécutable. Pour se prémunir contre le spoofing, ces fichiers ne devraient pas être en écriture pour les utilisateurs standards.

[3] Les fichiers .INI et les .PDF contrôlent l'installation et les actions d'applications, et ne devraient pas être en écriture pour le public pour se prémunir contre le spoofing. Nous sommes un peu soucieux quant à laisser des utilisateurs non administrateurs mettre en place des scripts qui installent du matériel, mais c'est acceptable pour le moment.

[4] Laissez le public installer des nouveaux curseurs et police semble sûre si l'on considère le fait que ces fichiers curseurs et police ne contiennent pas de code exécutable.

[5] Chaque sous répertoire de PROFILES contient un profil utilisateur. Le système gère convenablement et automatiquement cette arborescence et aucun modification n'est nécessaire.

[6] Enlevez les entrées Tout le monde et Opérateurs de Serveurs de ces arborescences. Les fichiers dans REPAIR peuvent contenir des Mots de passe cryptés qui ne devraient être accessibles qu'aux administrateurs globaux. Voir "Protection des Mots de passe cryptés & SYSKEY" dans *Stratégies Générales*.

[7] Nous n'autorisons pas les Opérateurs de Serveurs ou les Utilisateurs avec Pouvoirs à accéder aux fichiers dans TEMP parce que cela leur permet de lire et d'écrire sur n'importe quels autres fichiers utilisateurs, ce qui semble un laxisme non nécessaire. Toutefois, cela ne leur permet pas de supprimer les fichiers qui s'accumulent inévitablement dans \TEMP, et il semble peu sage de nécessiter une connexion administrative totale pour le vider. On peut autoriser des utilisateurs (ou un groupe) de confiance, spécifique pour supprimer (mais pas lire et écrire) tous les fichiers dans \TEMP.

[8] SYSTEM32 contient de nombreux fichiers de sécurité sensibles. Malheureusement, c'est aussi une grande décharge pour beaucoup d'applications qui créent des fichiers là quand elles ne savent pas où les mettre. Le système cherche dans ce répertoire des noms de DLL, et c'est seulement à cause du spoofing que le public ne devrait pas être autorisé à ajouter de nouveaux fichiers. La restriction de l'accès à ce répertoire entraînera inévitablement des problèmes de compatibilité. Les fichiers récemment ajoutés peuvent nécessiter des ACLs particulières.

[9] Les programmes de sauvegardes Windows NT créent généralement des fichiers temporaires ici. Les Opérateurs de Sauvegarde ont besoin de l'accès Modifier pour certains fichiers par accès par défaut.

[10] Ceci représente potentiellement des opportunités pour le spoofing. Au Niveau 2, nous recommandons que vous enleviez les entrées Installateurs d'Applications et Opérateurs de Serveurs, en laissant l'accès en écriture uniquement pour les administrateurs globaux. Notons qu'elles sont positionnées avec la permission Modifier pour Public par l'outil C2CONFIG .

[11] Par défaut les Opérateurs de Serveur ont le Contrôle Total ou Modifier sur ces arborescences, ce qui leur donne la capacité de tromper le système de sécurité. Donc nous excluons leur accès. Bien que cela puisse être tempéré pour les Opérateurs de Serveurs, Les Installeurs d'Applications ne devraient jamais être autorisés à installer de nouveaux pilotes.

[12] Ces Conseils n'abordent pas le sous système OS/2, et sans cette analyse, l'attitude la plus prudente est de mettre les fichiers dans cette arborescence sur Public: Lire.

[13] Nous continuons la pratique par défaut qui est de donner l'accès Modifier aux Utilisateurs avec Pouvoirs sur les éléments de cette arborescence. Quoiqu'il en soit, ceci peut être contraire à la stratégie de certains sites.

[14] Certains fichiers dans cette arborescence (comme NTCONFIG.POL, voir *Fichiers de Stratégies Système*) demande des ACLs plus strictes. A l'exception du partage NETLOGON, cette arborescence est essentiellement utilisée par le service Réplicateur et les ACLs des fichiers répliqués sont à la discrétion des administrateurs. Il semble plus raisonnable de donner aux Opérateurs de Serveurs la permission Contrôle Total (plutôt que Modifier) ce qui leur permet de gérer entièrement la Réplication.

[15] Gardez le complément APERCU RAPIDE dans ce répertoire. Ce répertoire doit donc être protégé comme s'il contenait un utilitaire d'administration, donc nous ne laissons pas les Installateurs d'Applications le gérer. Nous autorisons l'accès aux Opérateurs de Serveurs, bien que les systèmes de niveau 2 qui sont concernés par le spoofing puissent vouloir limiter cela puisqu'il est probablement peu utilisé.

[16] Quelques notes à propos des fichiers dans WINNT.

- CONTROL.INI n'est pas utilisé par NT.
- NETLOGON.CHG est présent seulement sur les contrôleurs de domaines et il est verrouillé à l'ouverture par le système.
- SETUP.OLD et SETUP.TXT sont d'une utilisation incertaine.

[17] Ceci est utilisé par les interfaces administratives et devrait seulement être sur Modifier pour les administrateurs.

[18] D'une utilisation incertaine sur Windows NT. Ce répertoire et ses fichiers peuvent avoir besoin d'un accès public sur Modifier.

[19] C'est un peu dangereux que de laisser les Installateurs ajouter de nouveaux exécutables dans des répertoires contenu dans le chemin de recherche DOS , comme WINNT et WINNT\SYSTEM32. Un script qui dénierai l'accès aux fichiers *.EXE dont le groupe local Administrateurs ne serait pas propriétaire serait appréciable.

[20] Enlevez ce répertoire du chemin de recherche administrateur.

[21] L'Administration DHCP du réseau va au-delà des tâches des Installateurs, donc ils n'ont aucun accès ici. Alors que ce serait peu dangereux de laisser l'accès aux Utilisateurs avec Pouvoirs , cela semble peu utile.

[22] L'Administration RAS du réseau va au-delà des tâches des Installateurs, donc ils n'ont aucun accès ici. Les Utilisateurs avec Pouvoirs n'ont pas d'accès car cela leur permettrait d'ouvrir leurs systèmes à l'accès réseau à distance.

[23] Ceci semble être un répertoire réseau, et l'accès y est donc interdit pour les Installateurs d'Applications.

[24] Activez cela seulement pour les fichiers de l'installation standard de Windows NT. Notez que seulement les administrateurs totaux peuvent modifier ou remplacer ces fichiers. On ne devrait réduire cela que pour des programmes utilisés par des Administrateurs "Pleins Pouvoirs". Pour les programmes non sûrs ajoutés par la suite, éviter l'accès administrateur en retirant la permission d'accès "X".

[25] Ces commandes sont pour les services de type UNIX “connexion à distance ”. Elles devraient être enlevées du système, et rajoutées seulement si cela s'avère nécessaire pour l'ordinateur client.

[26] L'idée générale est d’autoriser les Opérateurs de Serveurs à avoir le contrôle total de cette arborescence, alors que les Opérateurs d’Imprimantes et les Utilisateurs avec Pouvoirs ont seulement la capacité de Modifier.

[27] Ceci est le répertoire spool par défaut, de Windows NT. Toutefois, son emplacement peut être modifié en changeant l’entrée correspondante dans la Base de Registres, et cette ACL devrait être appliquée aux répertoires spool alternatifs. Cette configuration ne permet pas aux utilisateurs de lire les autres fichiers du spool. Le répertoire TMP peut être aussi utilisé pour des informations temporaires sur l’impression qui peuvent contenir des données utilisateurs et ses fichiers devraient donc être protégés. La configuration ACL pour les Utilisateurs avec Pouvoirs ne leur permet pas de lire les autres fichiers spool des utilisateurs, bien qu’ils puissent les effacer.

Paramètres d'ACL sur la Base de Registre

Le jeu de permissions utilisé ci dessous est :

Lire = QENR
Ajouter = QCENR
Modifier = QSCENDR

Pour référence, les permissions individuelles sont:

Q = Lire une valeur de clé (query value)
S = écrire une valeur de clé (set value)
C = créer des sous-clés (create subkey)
E = Lire le nom des sous-clés (enumerate subkeys)
N = recevoir une notification lors de la modification d'une clé (receive notification when key is modified)
D = suppression de la clé (delete the key)
R = lire l'ACL de la clé (Read key's ACL)

Les abréviations suivantes sont utilisées pour les groupes locaux:

Public = Tout le Monde
Installeurs = Installateurs d’Applications
SrvOps = Opérateurs de Serveur
PwrUsers = Utilisateurs avec Pouvoirs

Ces techniques qui empêchent l'accès non authentifié à la Base de Registres enlèvent le besoin d’utiliser Utilisateurs Authentifiés en tant qu'entrée Publique. De la même manière, il n'est pas évident qu'il y ait un changement significatif à utiliser Utilisateurs comme entrée Public, bien que ce soit potentiellement plus restrictif que Tout le Monde et qu'Utilisateurs Authentifiés. Si Utilisateurs ne pose pas de problème opérationnels, alors il pourrait être simplement utilisé.

Toutes les ACLs ci-dessous sont à inclure dans les entrées suivantes, ce qui est le standard pour la base de registres:

ACEs Communes dans toutes les ACLs de la Base de Registres

CREATEUR/PROPRIETAIRE Administrateurs SYSTEM	Contrôle Total

Toutes les autres clés de Registres apparaissent protégées convenablement comme installées pour les Niveaux 1 et 2.

☞ Modifiez les clés de la base de Registres qui suivent en enlevant les entrées du groupe Tout le monde de ces clés (si elles existent) et en les remplaçant avec les valeurs indiquées. Ne pas Modifier les ACLs des sous-clés sauf si le commentaire “Arbre entier” vous indique de le faire ainsi, et dans ce cas modifiez les ACLs de toutes les clés à la base de l'arbre de la clé en question. Exception faite, comme indiqué, de ne pas modifier les permissions pour les divers Opérateurs, Utilisateurs avec Pouvoirs, ou les autres groupes prédéfinis.

HKEY_LOCAL_MACHINE

\Software	Installeurs: Modifier Public: Lire	Voir note [1].
\Software\Classes	Installeurs: Ajouter Public: Lire	L'arborescence nécessite un traitement particulier. Voir note [13].
\Software\Microsoft\Windows \CurentVersion \App Paths	Installeurs: Modifier Public: Lire	Arbre Entier. Voir note [2].
\Software\Microsoft\Windows \CurentVersion \Explorer	Public: Lire	Arbre Entier. Voir note [3].
\Software\Microsoft\Windows \CurentVersion \Embedding	Installeurs: Modifier Public: Lire	Arbre Entier.
\Software\Microsoft\Windows \CurrentVersion \Run, RunOnce, and Uninstall	Public: Lire	Trois clés. Voir note [4].
\Software\Microsoft \Windows NT\CurrentVersion \AeDebug	Public: Lire	Arbre Entier. Voir note [5].
\Software\Microsoft \Windows NT\CurrentVersion \Compatibility	Installeurs: Modifier Public: Lire	Arbre Entier.
\Software\Microsoft \Windows NT\CurrentVersion \Font*, GRE_Initialize \Software\Microsoft \Windows NT\CurrentVersion \Type 1 Installer\Type 1 Fonts	Installeurs: Modifier Public: Ajouter Installeurs: Modifier Public: Add	Clés qui commencent par “Font,” excepté FontDrivers, et GRE-Initialize. Voir note [10].
\Software\Microsoft \Windows NT\CurrentVersion \Font Drivers	Public: Lire	Voir note [11].
\Software\Microsoft \Windows NT\CurrentVersion \Drivers, Drivers.desc	Public: Lire	Arbre Entier. Voir note [9].
\Software\Microsoft \Windows NT\CurrentVersion \MCI, MCI Extensions	Installeurs: Modifier Public: Lire	Arbre Entier.
\Software\Microsoft \Windows NT\CurrentVersion \Ports	INTERACTIVE: Modifier Public: Lire	Arbre Entier. Voir note [12].
\Software\Microsoft \Windows NT\CurrentVersion \WOW	Public: Lire	Arbre Entier. Voir note [6].
\Software\Microsoft \Windows NT\CurrentVersion \Profile List	Public: Ajouter*	ACE qui ne se propagent pas si possible. Voir note [7].
\Software \Windows 3.1 Migration Status	Public: Lire	Arbre Entier.
\System\CurrentControlSet \Services\LanmanServer\Shares	Public: Lire	Arbre Entier. Voir note [14].
\System\CurrentControlSet \Services	Public: Lire	Arbre Entier. Voir note [8].

HKEY_USERS \.DEFAULT

\Software\Microsoft \Windows NT\CurrentVersion \Program Manager \Common Groups	Installeurs: Modifier Public: Lire	

[1] Comme l'entrée pointe vers cet arbre, la clé Software devrait permettre aux seuls Installateurs d'Applications de créer des sous-clés.

[2] Vide à l'installation. Peut présenter la menace potentielle de spoofing, refusez de donner l'accès Public:Ecriture pour toutes les clés nouvellement ajoutées.

[3] Semble être inutilisé.

[4] La commande appelée dans la clé Run s'exécute à la connexion de tous les utilisateurs (y compris les administrateurs) et doit donc être protégée contre le spoofing. Elle ne devrait être en écriture que pour les administrateurs globaux. De la même façon, protégez RunOnce et Uninstall. (Se référer à [KBase Q126713], qui sont postérieurs à la découverte de ce problème durant cette étude.)

[5] Paramètres pour le debugger système que les utilisateurs peuvent exécuter quand un programme plante (comme "Dr. Watson"). L'accès est restreint pour réduire les opportunités potentielles de spoofing.

[6] Contient les paramètres pour l'environnement DOS. Bien qu'il ne soit pas évident de déterminer l'existence d'un risque de spoofing, il semble sage d'empêcher la modification Publique.

[7] Chaque sous-clé dans Profiles contient les paramètres pour un profile créé dans WINNT\Profiles. Pour empêcher le spoofing, une nouvelle sous-clé ne devrait pas être en écriture pour Public. Malheureusement, il n'y a pas d'outils standard pour les ACLs du Registre qui permette au public de créer des clés sur lesquelles il n'y a pas d'accès public, bien que la permission "Ajouter" est sûre tant que les sous-clés n'ont pas elles même de sous-clés significatives, ce qui est le cas dans Profiles. Les outils de sociétés tierces qui peuvent installer des entrées ACL qui ne se propage pas aux sous-clés[18] sont importants ici car ils produisent la sécurité désirée.

[8] Parce que seulement les administrateurs globaux peuvent installer des applications dans le gestionnaire de Service, mettre leurs paramètres ici peut sembler bénin. Toutefois, parce que les services s'exécutent communément sous le compte SYSTEM il semble préférable d'autoriser uniquement les administrateurs globaux à modifier les paramètres de service. Voir *Services Système*.

[9] Drivers32 est l'endroit principal de stockage pour les pilotes Windows NT, et il est fortement protégé. La fonction de la clé Driver n'est pas très claire, mais nous la protégeons tout de même.

[10] Certains sites désireront peut être restreindre l'accès Lecture Publique pour empêcher les utilisateurs d'ajouter des polices.

[11] Les fonctions des éléments dans FontDrivers ne sont pas clairs. Quoiqu'il en soit, il définira peut-être les emplacements de codes exécutables qui s'exécutent dans le système

[18] Super CACLS (http://www.TrustedSystems.com) est le seul que nous ayons trouvé dans nos recherches.

kernel, ce qui en fait un code extrêmement sensible. Nous protégeons fortement cette clé par sécurité.

[12] Les paramètres pour COM, LPT, et les autres ports. Nous autorisons les utilisateurs "INTERACTIVE" à les modifier parce qu'il semble qu'il y ait que peu de risque de sécurité, bien que certains sites désireront peut être réduire ces ACLs. Notez que [Micr97] préconise de réduire ces clés à Public: Lecture.

[13] Après l'installation de Windows NT, mettez les ACLS sur l'arbre Classes entier sur Public: Lire (ainsi que les ACEs communes), positionnez ensuite les ACLs sur les clés de Classes comme indiqué. (Ceci retire l'entrée INTERACTIVE de ces ACLs). Cet arbre de Registre contient diverses propriétés associées avec les applications, comme la corrélation entre l'extension d'un fichier et l'application définie pour le gérer. Il semble prudent de limiter ces clés car elles constituent des menaces de spoofing potentielles, bien que cela puisse avoir un impact sur certaines applications.

[14] Les valeurs dans cette clé et des sous-clés de Sécurité contiennent des informations sensibles à propos des partages répertoires et imprimantes. Ces valeurs sont protégées par défaut de façon adéquate. Toutefois, Public peut ajouter de nouvelles sous clés à ces clés, et le guide, tout comme [Micr97], préconise de les réduire comme indiqué plus haut.

Les notes suivantes décrivent les ruches générales de la base de registres et ne constituent qu'une information. Les ACL dans la partie **HKEY_LOCAL_MACHINE** (HKLM) varient considérablement. HKLM contient les arborescences: HARDWARE, SAM, SECURITY, SOFTWARE, et SYSTEM. La sous-arborescence HARDWARE est complètement recréée à chaque démarrage pour correspondre au matériel système détecte durant le démarrage. La sous-arborescence SAM contient les comptes utilisateurs et elle est protégée contre tout accès. Quoiqu'il en soit, les administrateurs globaux peuvent Modifier ces ACLs et donc accéder à cette arborescence. Les comptes sont cryptés et un tel accès est sans intérêt. SECURITY\SAM et SAM\SAM sont le même objet. (L'un est lié à l'autre.) L'arborescence SAM est stockée dans le fichier CONFIG\SAM dans WINNT\SYSTEM32. L'arborescence SECURITY stocke différentes stratégies (comme stratégies de droit et d'audit), et elle est stockée dans le fichier CONFIG\SECURITY dans WINNT. Il est aussi crypté. SOFTWARE contient de nombreux paramètres d'applications indépendantes de l'utilisateur et elle est stockée dans CONFIG\SOFTWARE. SYSTEM contient les informations non-volatiles de configuration du système et elle est stockée dans CONFIG\SYSTEM, et CONFIG\SYSTEM.ALT est une copie de secours de ce fichier.

La partie **HKEY_CURRENT_ USER** (**HKCU**) contient les paramètres qui s'appliquent à un utilisateur connecté localement. Dans le mode profile normal, le système sauvegarde cette partie à la déconnexion et la restaure à la connexion au fichier de profile local ("###" est un nombre choisi par le système pour rendre le profile unique, bien qu'il puisse être absent):

```
WINNT\Profiles\NAME### \NTUSER.DAT
```

Le public n'a pas accès à HKCU – seulement ses utilisateurs et ses administrateurs. La sous-arborescence HKCU suivante:

```
HKCU\Software\Microsoft\Windows\CurrentVersion\Policies
```

permet à l'utilisateur actuel d'avoir un accès Lecture. Le système utilise cette arborescence pour les paramêtres destinés à restreindre l'utilisateur d'une manière qu'il ne peut réduire.

La ruche **HKEY_USERS** inclut une sous-arborescence .DEFAULT que le système utilise pour les programmes qui ont besoin de ses paramètres mais qui n'ont pas de session

connexion. Il contient aussi une arborescence pour chaque utilisateur avec une session locale active, y compris l'utilisateur connecté (qui est lié à HKCU), et, par exemple, les utilisateurs fonctionnant à partir du service Planification.

Autres parties:

HKEY_CURRENT_CONFIG est un lien symbolique vers:

```
HKLM\System\CurrentControlSet\Hardware Profiles\Current
```

HKEY_CLASSES_ROOT est un lien symbolique vers:

```
HKLM\SOFTWARE\Classes
```

Installation et Tests de Nouvelles Applications

Ces Conseils prescrivent de "réduire" les ACLs sur différents fichiers, répertoires, et clés de la base de Registres de l'installation standard de Windows. L'effet contraire le plus probable est que les programmes échouent parce qu'ils ne peuvent pas modifier ces objets. Bien que le guide réduise seulement les zones que les applications ne devraient pas en principe modifier, il n'y a pas de standard absolu, et les applications non écrites spécifiquement pour Windows NT causent la plupart des problèmes. Il est donc important que vous testiez les logiciels nouvellement installés pour de telles erreurs. Installer de telles applications (à l'opposé de leur usage au jour le jour) peut aussi induire ces problèmes, et la technique d' d'enregistrement de sécurité décrite ci dessous est utile dans les deux cas.

Les applications correctement écrites pour Windows NT gardent les données spécifiques à un utilisateur dans un répertoire et dans des clés de la Base de Registres dédiées à cet utilisateur, par exemple leur répertoires personnels ou répertoires qu'ils peuvent designer dans l'application (habituellement sa fenêtre "Options"). Utilisées par des utilisateurs normaux (non-administrateurs), de telles applications, en général, ne créent et ne modifient pas les fichiers dans les répertoires d'installation ou la partie HKEY_LOCAL_MACHINE de la base de Registre.

Toutefois, il y a des exceptions. Quand vous installez une application, testez la complètement en l'exécutant en tant qu'utilisateur normal. Précisément, n'utilisez pas un compte qui est membre des groupes qui ont plus d'autorisations que l'accès "Tout le Monde" sur le répertoire d'installation de l'application. (Voir "Répertoires d'Applications " dans *Répertoires personnels & Application*.) Vous rencontrerez peut-être des erreurs si les programmes de l'application ne peuvent écrire sur un fichier, répertoire, ou partie de la Base de Registres. Ces erreurs n'arrivent pas normalement quand vous exécutez les programmes à partir d'un compte qui est membre du groupe Installateurs d'Applications.

Si vous voulez que les utilisateurs communs puissent utiliser des fonctions qui sont bloquées par de telles erreurs, vous devez donner un "R" et peut être d'autres permissions pour les ACLs sur les objets limitants. Quoiqu'il en soit, un mot de prudence: ceci peut permettre à un utilisateur d'affecter ou de compromettre le travail d'un autre. Bien qu'il puisse être difficile de détecter ces situations, vous ne devriez pas essayer de le faire. Vous pourrez peut être donner plus de permissions uniquement aux utilisateurs dont vous êtes sûr qu'ils n'en abuseront pas.

Vous pouvez utiliser le journal de sécurité pour déterminer quels fichiers ou clés de la base de registres produisent ces erreurs. Configurez l'information d'audit sur le système de fichier et l'arbre du Registres pour enregistrer les échecs de modifications "en écriture" sur le compte qui produit les erreurs. (Vous avez besoin du Droit de "Gérer l'audit & journal sécurité" pour le faire.) Assurez-vous que la stratégie d'audit permet les échecs dans la catégorie "Accès aux

fichiers et Objets", bien que seulement les administrateurs globaux puissent modifier cette stratégie. Examinez le journal de sécurité pour les erreurs. Il y a trois arborescences où vous avez le plus de chance de trouver des objets qui peuvent causer ces erreurs:

- L'arborescence du répertoire principal d'installation de l'application.
- L'arborescence du répertoire racine du système, généralement appelée WINNT.
- L'arborescence émanant de la clé de la Base de Registres dans HKEY_LOCAL_MACHINE\Software est nommée par la compagnie ou l'application, que les applications Windows NT créent souvent pour garder les données indépendantes de l'utilisateur.

Chapitres Associés:

Répertoires personnels & application

Variable "PATH" et autres variables d'environnement

Références:

Un document complémentaire à cette étude résume les paramètres d'ACL en prenant considération de configurations courantes :

[Sutt96] Chapitre 4, *ACLs*, p. 159.

[Navy97] [Micr97]
Elles présentent toutes les deux les configurations ACL basées sur l'outil C2CONFIG.

[RKitS] Chapitre 24, *Editeur de Base de Registres et Administration de la Base de Registres*. Une vue globale de la gestion de la Base de Registres.

8. Applications & Répertoires Utilisateurs

A cause des dommages considérables que peuvent causer des programmes malintentionnés, il est important que vous contrôliez strictement leur introduction sur le système, protégez leurs différents fichiers exécutables et données de modifications injustifiées, et essayez de vous assurer que les utilisateurs avec des capacités sensibles n'exécutent pas des applications dangereuses. (Une application en qui les administrateurs savent qu'elle n'est pas malintentionnée est appelée application de "confiance").Pour servir ces buts, stockez les applications tierces dans les répertoires "officiels" sous le contrôle d'utilisateurs dignes de confiance. Ceci fournit une utilisation plus cohérente des ACLs.

Les répertoires qui contiennent des programmes généraux (fichiers *.EXE) sont souvent appelés les répertoires "BIN". Considérez un répertoire BIN comme un répertoire d' applications. La principale différence est que vous créez rarement des sous-répertoires par programmes dans les répertoires BIN.

Le groupe Installateurs d' Application se voit fournir un accès spécial à ces répertoires pour qu'il puisse ajouter de nouvelles applications. Cela est lié à leurs capacités à modifier des éléments d'installation dans le répertoire WINNT et la Base de Registres.

Un nouveau groupe "Utilisateurs d' Application "permet d'empêcher les utilisateurs sensibles, comme les administrateurs globaux, d'exécuter des applications à moins que ces applications soient jugées dignes de confiance. Utilisateurs d' Application contient tous les Utilisateurs qui sont autorisés à utiliser les applications locales *à l'exception* des comptes administratifs sensibles.

Voir la discussion sur le groupes installateurs d'applications dans l'aperçu pour *Système de Fichier et Paramètres d'ACL du Registres.*

Conseils

Répertoires d' Applications

Niveau 1 & 2:

Les pratiques suivantes sont *recommandées*. (Notez que le groupe Installateurs d' Applications est aussi *recommandé,* et non pas prescrit.)

- Créez un ou peu de répertoires officiels pour les applications, par exemple, un seul appelé "C:\Program Files," qui est le standard lors de l'installation de Windows NT. Minimisez le nombre de répertoires d'applications. Vous installerez généralement chaque application dans son propre sous-répertoire dans l'un des répertoires d'applications, bien que certaines suites d'applications partagent un seul et même sous-répertoire.
- Donnez à ces répertoires les ACLs suivantes (y compris les fichiers et répertoires de leurs arborescences, si déjà installés):

C:\Program Files …*et/ou autres répertoires programme*

Utilisateurs d' Application	Lecture [1]
Installateurs d' Application	Modifier
Administrateurs	Contrôle Total [2]
SYSTEM	Contrôle Total [2]
Opérateurs de Serveurs	Contrôle Total [2]

[1] "Utilisateurs d' Application " se réfère au groupe dont les membres doivent utiliser les applications. Parce que nous excluons pour les administrateurs l'exécution de fichiers *.EXE,

nous ne pouvons utiliser aucun groupe dont les administrateurs sont membres, comme Tout le Monde et Utilisateurs.

[2] Utilisez les Opérateurs de Serveurs uniquement sur les contrôleurs de domaine. Ne les remplacez pas par des Utilisateurs avec Pouvoirs sur les stations de travail NT.

- Pour n'importe quelle arborescence d'applications pre-installées, modifier tous les fichiers *.EXE pour enlever la permission "R" pour les utilisateurs d' Application. Les Installateurs d'Application devraient faire cela après avoir installé chaque application. Voir "Retirer le "R" des Fichiers Programmes dans Spoofing".
- Pour n'importe quelle arborescence d'applications pre-installées, modifier tous les fichiers *.EXE pour enlever la permission "X" pour les Installateurs d'Applications, les Administrateurs, Opérateurs de Serveur, et SYSTEM. Les Installateurs d'Application devrait le faire après l'installation et le test de chaque application. Les fichiers *.EXE que vous estimez "dignes de confiance" peuvent être exemptés s'il est important que ces groupes administratifs puissent utiliser les programmes.

Vous n'avez pas besoin de modifier ces ACL dans les répertoire des application nouvellement installées à moins que l'application ne le nécessite. Voir "Installer & Tester de Nouvelles Applications" dans *Système de Fichiers & Paramètres d'ACL du Registre*.

Répertoires personnels

Chaque utilisateur qui se connecte à un ordinateur et qui a besoin d'un espace de travail sous son contrôle doit avoir un répertoire personnel sur cet ordinateur. Les utilisateurs ne devraient pas avoir accès à un répertoire personnel avant que son propriétaire n'ait eu le temps de personnaliser sa structure d'ACL.

Nous traitons aussi les répertoires personnels partagés par les utilisateurs. L' essence de ce partage est que par défaut chaque utilisateur doit s'attendre à des protections limitées par rapport aux autres utilisateurs qui partagent ce répertoire. Tant que les utilisateurs comprennent ceci, les répertoires personnels partagés ne sont pas déconseillés même au Niveau 2.

Niveaux 1 & 2:

Les pratiques suivantes sont *recommandées*.

- Créez un répertoire appelé USERS sur chaque lecteur logique pour contenir les répertoires personnels avec les mêmes ACLs que celles recommandées pour la racine du répertoire du lecteur (*voir Système de Fichier et Paramètres d'ACL du Registre*). C:\USERS est l'endroit habituel.
- Créez un répertoire pour chaque utilisateur avec un nom de répertoire basé sur le nom de connexion de l'utilisateur. (Notez qu'il peut y avoir des utilisateurs de différents domaines avec le même nom de compte, et vous aurez peut-être besoin de les distinguer entre eux, typiquement en préfixant le nom de domaine où les conflits existent.) Appliquez les ACLs suivantes, où "*nom d'utilisateur* " est le nom du compte.

C:\Users *nom d'utilisateur* … et/ou autre répertoires personnels

Nom d'utilisateurs	Contrôle Total
CREATEUR/PROPRIETAIRE	Contrôle Total
Gestionnaires de Données Utilisateurs (opt)	Contrôle Total
Administrateurs	Contrôle Total
SYSTEM	Contrôle Total

Gestionnaires de Données Utilisateurs est optionnel et représente n'importe quel groupe qui par stratégie se voit donner par défaut l'accès contrôle total aux données utilisateurs. Vous pouvez utiliser aussi des groupes comme Opérateurs de Serveur. Les utilisateurs peuvent par la suite exclure ce groupe. Ne donnez pas à de tels groupes le Droit de Prendre Possession car cela leur permettrait de modifier tous les fichiers sur le système.

- Si un répertoire personnel doit être partagé par d'autres utilisateurs, remplacez la première entrée ACL au dessus par une entrée de la forme suivante pour chaque utilisateur:

  Nom d'utilisateur Accès Spécial (RWXD)*(Non Spécifié)

  Ceci autorise chaque utilisateur à créer de nouveaux éléments qui par défaut ne donnent aucun droit aux autres utilisateurs. (Le "*" indique que cette entrée devrait être installée comme une entrée non-propageante si vous n'avez pas d'outils pour le faire.)

- Si le répertoire doit être partagé par un groupe, utilisez la même entrée en substituant le groupe comme le *compte_utilisateur* avec les permissions suivantes:

  Nom du groupe Accès Spécial (RWXD)*(Non Spécifié)

  Ceci permet à chaque utilisateur de créer de nouveaux éléments auxquels les autres utilisateurs n'ont pas accès.

- Installez le répertoire de base dans le compte utilisateur du Gestionnaire des Utilisateurs.
- Facultativement, créez un répertoire USERS\DEFAULT pour les utilisateurs qui n'ont pas de répertoires personnels sur cet ordinateur. Ce répertoire est quasiment le même que C:\TEMP excepté que les utilisateurs ont une plus grande certitude de permanence.
- Alternativement, vous pouvez créer un répertoire de base sur un répertoire distant partagé. Utilisez les mêmes techniques d'ACLs.

Ce guide met en avant la pratique standard qui permet aux groupes Administrateurs et SYSTEM d'avoir un contrôle total sur tous les fichiers et dossiers dans les répertoires personnels. Les utilisateurs peuvent enlevez ces groupes de leurs propres ACL, mais cela peut rendre les opérations plus difficiles en forçant les administrateurs à prendre possession dans des cas exceptionnels où ils ont besoin de résoudre des problèmes dans les arborescences du répertoire utilisateur.

Examen Régulier:

L'examinateur devrait formuler une stratégie de site pour les répertoires personnels utilisateurs, revoyez alors tous les répertoires personnels à la recherche de pratiques potentiellement dangereuses vis-à-vis de votre stratégie. Ce qui suit sont des exemples qui peuvent être inclus dans une telle stratégie:

- Les fichiers personnels qui contiennent des informations "secrètes", comme les mots de passe pour différentes applications, doivent être correctement protégés, ou, de préférence, enlevés. En aucun cas les utilisateurs ne doivent stocker un mot de passe de connexion Windows dans un fichier.

- Renforcer la stratégie du site comme si les utilisateurs non-administratifs importaient des programmes sur le système. Si ils sont autorisés, les fichiers exécutables et leurs DLLs doivent être protégés de la modification.
- Vérifier les cas où des individus ne protègent pas correctement les arborescences de leurs répertoires personnels.
- Vérifier les cas où des individus partagent un répertoire personnel mais dont l'un des utilisateur stocke des données pour lesquelles les autres ne sont pas autorisés à accéder de par la stratégies du site.

Sections Associées:

Système de Fichier & Paramètre d'ACLs du Registre, y compris "Installer & Tester des Nouvelles Applications"

Spoofing, les dommages que les applications malintentionnées peuvent faire

Droits Utilisateurs, le droit d'Outrepasser le Contrôle de Parcours

9. Comptes d'Utilisateurs & Groupes

Ce guide contient des recommandations pour différents réglages dans les comptes utilisateurs, et quelques recommandations générales pour créer des groupes d'utilisateurs.

Conseils

Comptes d'Utilisateurs

Ce guide contient différentes stratégies en rapport avec les comptes utilisateurs définis dans les différentes fonctions du menu du Gestionnaire des Utilisateurs, à l'exception des stratégies couvertes par le chapitre Mots de Passe. Ce guide ne prescrit aucune considération de sécurité pour les boutons Groupes ou Profil. Voir *Service d'Accès Distant* pour une discussion sur le bouton "*Numérotation*".

Niveau 1:

- Appliquez les Conseils suivants aux paramètres de chaque nouveau compte que vous créez:

  Profile: Pas prescrit pour la sécurité. Quoiqu'il en soit, les scripts à la connexion et les informations de profiles ne devraient être accessibles qu'à l'utilisateur concerné et aux administrateurs.

  Heures: Pas prescrit. (Voir les notes plus bas.)

  Se Connecter A: Nous *recommandons* que vous configuriez ceci de façon raisonnablement serré, à moins que vous n'ayez limité la connexion en utilisant le Droit de "Se connecter localement." (Voir les notes plus bas.)

  Compte: Ce guide ne prescrit pas de durée de vie spécifique pour des raisons de sécurité, mais les comptes avec une durée de vie désirée limitée devrait être configurés de manière correspondante.

- Désactivez les compte Invité (sélectionnez "Compte Désactive" dans la fenêtre principale de compte). Pour plus d'assurance, donnez lui un long mot de passe aléatoire que vous ne conservez pas, configurez ses heures de connexion à aucune, ne l'autorisez à se connecter à des stations de travail, et mettez sa date d'expiration à une date passée.

Niveau 2:

- Appliquez les Conseils du Niveau 1, excepté:

  Heures: Nous *recommandons* que vous configuriez les heures de connexion de façon raisonnable. Quoiqu'il en soit, même au Niveau 2, il y' a peu de raisons d'incommoder vos utilisateurs de manière significative avec des temps restrictifs qui ne seraient pas raisonnables.

  Se connecter A: Configurez cette option aussi strictement que possible, à moins que vous n'ayez contrôlé la connexion en utilisant le Droit de "Se connecter localement." (Voir "Droits de Connexion dans les Environnements Multidomaines " dans *Domaines & Restrictions d Accès de Base*).

Examen Régulier:

- Vérifiez les comptes activés et qui ne servent plus.

- Assurez-vous que les limitations “Se Connecter A ” soient suffisamment strictes.

Groupes d’Utilisateurs

Cette courte partie couvre les groupes utilisateurs autres que les groupes administratifs et les groupes communs comme Utilisateurs et Utilisateurs de Domaines (voir Droits à la Connexion dans des Environnements Multidomaines ” dans *Domaines & Restriction d'Accès de Base*).

Niveaux 1 & 2:

- N’ajoutez pas les utilisateurs ou les groupes globaux dans le groupe Réplicateurs sur les contrôleurs de domaines.
- Le groupe “Invité” n’active pas les connexions non authentifiées comme le compte Invité le fait. Ce groupe ne nécessite donc pas d’attention spéciale. Comme tout groupe général, son utilisation dépend des utilisateurs qui en sont membres. Définissez et distribuez votre stratégie de site concernant l'utilisation du groupe Invité.
- Notez que les membres du groupe local Utilisateurs peuvent créer leur propres groupes. Si vous désirez limiter ceux qui peuvent créer des groupes, enlevez-les du groupe Utilisateurs (bien qu’ils puissent avoir des difficultés à accéder à certains objets). Le fait de créer des groupes étend les capacités de chacun, et nos conseils ne prescrivent pas de limiter son utilisation.
- Vous pouvez utiliser les groupes pour sélectionner un grand nombre d’utilisateurs pour les contrôles de sécurité, par exemple les heures de connexion, les Droits, et pour renouveler les mots de passe de force. Tandis que ce guide ne prescrit pas cette technique, vous trouverez peut-être que cela améliore votre capacité à gérer les paramètres de sécurité des comptes.

Examen Régulier:

- Surveillez continuellement les membres des différents groupes en cherchant les utilisateurs que l'on ne devrait pas trouver dans ces groupes. Le problème est que les utilisateurs donne l'accès aux groupes sur leurs objets en se basant sur leur idée de qui sont les membres du groupe ou qui ils seront plus tard. Par exemple, le fait d’inclure les utilisateurs dans un groupe nomme “BulldogProject” alors que certains n'ont aucun lien avec le projet constitue une erreur d'appréciation.

Notes

Il est souvent plus pratique de limiter les connexions locales à l’aide du bouton “Se Connecter A” que par la stratégie de Droits parce que les comptes de domaine sont gérés centralement sur les contrôleurs de domaine, tandis que la stratégie de Droits doit être maintenue sur chaque ordinateur. (Voir *Droits de l’Utilisateur*.)

Le fait de limiter les heures de connexion peut servir à empêcher les utilisateurs en qui vous avez le moins confiance d’utiliser le système pendant des heures où leurs activités ne peuvent être surveillées. Alors que cela peut essayer d'empêcher l’utilisation d’un mot de passe volé, nous ne jugeons pas que cela soit significatif en terme de sécurité. Tout bien considéré, sur la plupart des sites nous n’avons pas l’impression que les heures de connexion soient une protection efficace contre les attaques, et nous vous suggérons de délaisser un peu les heures de connexion en faveur de considérations opérationnelles, même au Niveau 2.

On s'intéressera peut-être à limiter la durée de vie d'un compte dans la possibilité où un administrateur ne gère pas correctement ou ne revoit pas régulièrement la base de données des comptes. Par exemple, les administrateurs peuvent oublier d'enlever un utilisateur qui a quitté le site. Quoiqu'il en soit, n'importe quelle limitation pourrait toujours offrir suffisamment de temps pour une attaque sur un tel compte.

Chapitres et Sections Associés:

Mots de passes

Droits Utilisateur, pour les Droits locaux et a distance

"Droits a la connexion dans les Environnements Multidomaines " dans *Domaines & Restrictions d'Accès de Base* pour l'utilisation générale des Droits a la connexion

Le Compte "Administrateur" dans *Structure Administrative*

Références:

[Sutt96] "Comptes" au Chapitre 7, *Gérer des Groupes et des Comptes*, p. 161-168.

10. Mots de Passe

Ce guide recommande divers paramètres qui gouvernent l'utilisation des mots de passe utilisateurs et administratifs. Le verrouillage de comptes est prescrit tant au Niveau 1 qu'au Niveau 2. Ce chapitre décrit des schémas de mots de passe et quantifie la probabilité de détermination de ces schémas. Cependant, les nécessités des sites concernant les paramètres des mots de passe, leur complexité et leur durée de vie, sont trop divers pour tenter une recommandation explicite. A la place, chaque site devra formuler sa propre stratégie basée sur une variété de facteurs.

Conseils

Niveaux 1 & 2:

Complexité des Mots de Passe et Durée de Vie

Chaque site devra formuler ses propres critères pour la complexité des mots de passe ((“Taille Minimale des Mots de Passe” dans la Stratégie de Compte) et durée de vie (“Age Maximum des Mots de Passe”). Vous devriez déterminer ceci en prenant en considération une estimation probabilistique de compromission d'un mot de passe comme nous le montrons en exemple dans “Attaques par Tentatives de Login” et “Attaques par Mots de Passe Capturés ,” ci-dessous. Le paramètre important est la probabilité qu'un mot de passe puisse être deviné durant sa durée de vie – en opposition à la simple taille de mots de passe.

Verrouillage par Mots de Passe

Positionnez le Verrouillage de mots de passe dans la stratégie de compte. Les mots de passe créés pour résister aux Attaques par Tentatives de Login (ci dessous) devraient avoir les paramètres de verrouillage à partir des tables ci-dessous. Nous *recommandons* que les mots de passe dont la complexité est créée pour les Attaques par Capture aient les paramètres suivants:

Verrouillage après	5 erreurs d'ouverture de session
Reset après	30 minutes
Verrouillé pendant	30 minutes

Les Mots de Passe conçus pour les Attaques par Capture sont de loin plus complexes que ceux adaptés pour les Tentatives de Login et le verrouillage n'a aucun intérêt pour contrer une attaque. Il est donc moins important d'ajuster finement ses paramètres.

Conseils pour les Utilisateurs qui définissent leurs propres Mots de Passe

Positionnez les paramètres suivants pour les utilisateurs qui choisissent leurs mots de passe :

- Activez l' “Unicité du Mot de Passe” dans la Stratégie de Compte pour mémoriser la valeur maximale (actuellement 24).
- Mettez l'âge minimum des mots de passe dans la Stratégie de Compte à 2 jours. Ceci décourage de tourner à travers une liste de mots de passe pour atteindre un ancien favori.(Il y a une grande latitude dans la valeur que vous pouvez prendre, mais 2 jours signifie que 48 jours doivent s'écouler avant qu'un utilisateur ne puisse revenir à un mot de passe préféré, et même ainsi seulement après 23 autres mots de passe.)

- Lorsque vous créez un compte pour un tel utilisateur, sélectionnez “L'utilisateur doit changer son Mot de Passe à la prochaine ouverture de session” (mais pas le point qui suit).
- Utiliser “L'Utilisateur doit ouvrir une session pour changer son mot de passe” pour éviter que les utilisateurs n'obtiennent un nouveau mot de passe une fois que leur ancien a expiré. Cependant, ceci les empêche aussi de changer leur mot de passe à la première connexion comme présenté dans le point précédent.
- Nous *recommandons* que vous mettiez l'option “Déconnectez les utilisateurs distants du serveur quand l'heure de connexion expire”. Ceci évite que les utilisateurs établissent de nouvelles sessions en dehors de leurs heures régulières.
- Créez votre Stratégie pour les mots de passe des comptes correspondants comme décrit dans “Mots de passe pour les Comptes Locaux Correspondants,” ci-dessous.
- Nous vous *recommandons* de tester une sélection de logiciels de "recherche de mot de passe" pour Windows NT régulièrement pour déterminer les comptes "faibles".[19] (Il n'y a pas de tels programmes dans la distribution de Windows NT, cependant des sociétés tierces peuvent les fournir.[20])

Mots de Passe définis Administrativement

Vous pouvez décider de laisser les administrateurs sélectionner les mots de passe pour tout ou partie des utilisateurs. Les utilisateurs insouciants peuvent prendre des mots de passe fragiles quoi que vous fassiez, et le seul moyen de garder des mots de passe solides est que vous les assigniez. Vous pouvez déterminer le mot de passe conjointement avec l'utilisateur afin d'être certain qu'il est à la fois simple à retenir et judicieux. Ceci est *recommandé* au Niveau 2 sauf si cela va à l'encontre de votre stratégie de site. Sélectionnez l'option “L'utilisateur ne peut pas changer le mot de passe” dans la fenêtre principale de compte pour chaque utilisateur en question.

Certains sites ont pour politique que les administrateurs ne puissent pas connaître les mots de passe des utilisateurs. Ces conseils ne vont pas à l'encontre de telles stratégies. Cependant, n'oubliez pas que les utilisateurs n'ont pratiquement aucune protection contre un Administrateur et très peu contre un Opérateur de Compte.

Filtrage de Mots de Passe

Ce Guide *recommande que vous* implémentiez un filtre de mots de passe qui applique rigoureusement votre stratégie. Reportez-vous à *Filtre de Mots de Passe* plus bas. Malheureusement, vous devez soit écrire le votre ou en acheter un. Nous ne recommandons ou ne dissuadons pas l'utilisateur d'utiliser le filtre Windows NT nommé "PASSFILT.”

Délai d'avertissement pour les Mots de Passe

Par défaut, Windows NT commence à avertir un utilisateur de l'expiration de son mot de passe 14 jours avant. Vous pouvez modifier cette valeur en ajoutant une valeur de type

---

[19] Un désavantage potentiel pour l'utilisation de ces vérificateurs de mots de passe et que si un "agresseur" sait que vous en utilisez un , ils peut éliminer tous les mots de passe interdits pour ses attaques en force brute ce qui peut accroître de manière significative ses chance de succès.

[20] Un outil nommé “L0phtcrack” est très populaire. Vous trouverez beaucoup d'informations à son sujet sur le Web.

REG_DWORD appelée “PasswordExpiryWarning,” dont le contenu spécifie le nombre de jours avant expiration:

```
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\
   CurrentVersion\Winlogon
```

Examen Régulier:

L'examen le plus important est de s'assurer du caractère aléatoire des mots de passe choisi par les utilisateurs.

Notes

Attaques par Tentatives de Login

La probabilité pour qu'un agresseur puisse deviner un mot de passe dépend étroitement de la vitesse à laquelle il peut tester des mots de passe et de la taille de ces derniers. Le taux de détermination dépend du type d'attaque et nous en présentons deux : tentatives d'ouverture de session et mots de passe capturés.

Dans une attaque par tentatives de login, l'agresseur tente de deviner un mot de passe en essayant une ouverture de session légitime, soit primaire via le clavier, soit secondaire via une source réseau. Nous supposons que le verrouillage de compte est mis en place. Les paramètres de verrouillage sont donc le facteur dominant dans le taux de détermination correcte d'un mot de passe et ainsi la probabilité qu'il a d'être deviné.

Le tableau de Tentatives d'ouverture de session ci-dessous montre la probabilité qu'un agresseur détermine un mot de passe sous le scénario en question et pendant sa durée de vie et ce pour trois niveaux de verrouillage (les trois colonnes de droite) pour différent types et taille de mots de passe (les lignes du bas). Le tableau inclut 5 différents types de mots de passe:

Aléatoire, alphabétique minuscule: Caractères de l'alphabet sélectionnés au hasard, minuscules (de “a” jusqu'à “z”), tels que “hqisgt” ou “oxdye.”

Alphanumériques aléatoires: Similaire mais sélectionnés aléatoirement à partir de chiffres (0-9) et de lettres alphabétiques minuscules et majuscules, par exemple “Hs6tY8.”

C-V-C-V-C: Mots de passes ”Prononçables” de la forme consonne-voyelle-consonne-voyelle-consonne, à partir de caractères alphanumériques minuscules, par exemple “misoq” ou ”paxun.”

C-V-C-C-V-C: Similaire mais avec une consonne en plus au milieu, un exemple serait “mistoq” ou ”paxlun.”

Abréviation de Phrase: Mots de Passe en minuscule construits par la concaténation du premier ou des deux premiers caractères d'un phrase sans aucune signification, comme “afeyc” à partir des premières lettres des mots de “allow fish eat yellow car.” (Il semble plus simple de se rappeler d'une phrase que l'on peut 'visualiser'.) Ces probabilités sont approximatives car certains caractères alphabétiques sont plus souvent choisis que d'autres. Le tableau divise l'ensemble théorique par deux (estimation globale) tenir compte des cas non aléatoires.

Ces recommandations n'entendent pas vous limiter à ces schémas. Cependant, si vous choisissez une autre solution, vous devriez calculer ses probabilités et les rapprocher avec les indications qui suivent.

Nous supposons que le taux le plus élevé pour le test de Mots de passe est environ un de moins que le seuil de verrouillage (la valeur “Réinitialiser le compteur après”) divisé par le temps de remise en activité. Ceci est accompli en testant un mot de passe de moins que la valeur seuil (pour éviter le verrouillage) et en attendant la période de remise à zéro du compteur. La durée de verrouillage n'a aucun effet dans ce cas parce que l'agresseur n'active jamais le verrou. A partir de l'idée de limiter le taux d'ouverture de sessions, vous pouvez sélectionner la plus petite durée de verrouillage permise qui est égale au seuil.

Le tableau montre les chances de trouver des mots de passe de différentes longueurs (la colonne “Taille”) avec un seuil de verrouillage (“Verrouiller après”) de 7 et un temps de remise à zéro (“Remise à zéro du compteur après”) de 5, 30, et 60 minutes. Une valeur de “probabilité” telle que 2 947 signifie que la possibilité est de “une pour 2 946” qu'un agresseur puisse deviner le mot de passe en tentant une connexion locale ou distante au taux maximal permit par les paramètres de verrouillage à travers le temps, dans ce cas un mois. La colonne “Espace” montre le nombre total de combinaisons pour un schéma donné de mot de passe. Vous pouvez ajuster ces valeurs pour différentes durée de vie de mot de passe en divisant la probabilité par la durée de vie en mois.

Tableau des Classes de Mots de passe - Tentatives d'ouverture de session

Durée de vie des mots de passe, mois				1	1	1
Seuil ("Verrouillage après")				7	7	7
Durée de Verrouillage ("activation après"), min				5	30	60
	Taille	**Espace**		**Probabilité**	**Probabilité**	**Probabilité**
Aléatoire, alphabétique minuscule	4	5.E+05			57	113
	5	1.E+07		246	1 473	2 947
	6	3.E+08		6 385	38 308	76 616
	7	8.E+09		166 001	996 008	1 992 016
C-V-C-V-C		4.E+05			54	109
C-V-C-C-V-C		1.E+07		236	1 417	2 833
Alphanumérique aléatoire	4	1.E+07		305	1 832	3 665
	5	9.E+08		18 935	113 608	227 215
	6	6.E+10		1 173 947	7 043 680	14 087 360
	7	4.E+12		72 784 693	436 708 160	873 416 321
	10	8.E+17		2.E+13	1.E+14	2.E+14
	14	1.E+25		3.E+20	2.E+21	3.E+21
"fish ate blue house"	4	2.E+05			28	57
	5	6.E+06		123	737	1 473
	6	2.E+08		3 192	19 154	38 308
	7	4.E+09		83 001	498 004	996 008

Ces classes de mots de passe sont basées sur la supposition que l'attaque s'effectue au travers du processus normal d'ouverture de session locale ou distante qui active le verrouillage. Le

compte local Administrateur n'est pas soumis au verrouillage et notre guide en parle particulièrement dans la section “Le compte Administrateur” dans *Structure Administrative*. Il y a aussi un moyen d'attaquer les mots de passe via leur endroit de stockage local que l'on gère avec des méthodes différentes, bien que des mots de passe plus complexes aident (voir “Protections des Mots de passe cryptés & SYSKEY” dans *Stratégies Générales*).

Attaques par Mots de Passe Capturés

Windows NT stocke une version cryptée du mot de passe, et si quelqu'un connaît l'algorithme de cryptage Windows NT (et il semble largement connu) alors l'on peut tenter une attaque par force brute. Les Attaques par capture du mot de passe se sont montrées effectives pour le cas où les mots de passe sont tirés d'une source locale de stockage. Heureusement, ceci peut être protégé. (Voir “ Protections des Mots de passe cryptés & SYSKEY ” dans *Stratégies Générales*.)

Cependant, il y' a des cas ou des écoutes actives ou passives peuvent voir le trafic d'authentification et appliquer des attaques en force brute ou par dictionnaire sur un mot de passe crypté. Par exemple, supposez qu'un schéma challenge-réponse envoie la séquence de challenge et de réponse en texte clair, et que la réponse calculée est une fonction connue du mot de passe utilisateur. Bien que le mot de passe en lui même n'ai jamais transité à travers le réseau, un agresseur peut porter une attaque en force brute en connaissant la séquence de challenge et sa réponse. Ces attaques fonctionnent à la vitesse permise par la puissance des ordinateurs et peut être très élevées. Il y a eu de nombreuses discussions publiques relatives à la capture de mots de passe en écoutant le trafic d'authentification.

Un réseau dont les mots de passe sont “exposés” est concerné par l'attaque ci-dessus. La première condition est que les mots de passe sont transmis d'une façon qui permet cette attaque, par exemple la séquence challenge-reponse cité ci-dessus. La seconde est que des programmes malveillants sur le réseau puissent lire le trafic brut de paquets sur le réseau. Ceci arrive quand des programmes sont utilisés sur des (1) systèmes d'exploitation sans protection du noyau, comme DOS, Windows (excepté Windows NT) et l'OS Macintosh , ou (2) des systèmes d'exploitation à noyau protégé qui sont mal administrés. Ceci couvre le cas où un agresseur puisse mettre un ordinateur de son choix sur le réseau. Le réseau Internet peut certainement être qualifié de réseau à mots de passe exposés.

Le tableau suivant montre la probabilité qu'un mot de passe capturé puisse être déterminé durant sa durée de vie. Il utilise un sous-ensemble des types de mots de passe ci-dessus, en omettant ceux qui ne sont pas efficaces. Il suppose qu'un agresseur peut effectuer plus de 1000 tentatives par secondes et une durée de vie de 1 mois. (Bien que certains lecteurs font remarquer que ce taux peut-être beaucoup plus important.) Comme avant, une “probabilité” de 2 947 signifie que les chances sont de “une pour 2 946” pour que le mot de passe soit deviné durant sa durée de vie. (Une valeur de 0 signifie que le mot de passe sera déterminé avec succès.) Vous pouvez adapter cela à différentes durées de vie du mot de passe en divisant la probabilité par la durée de vie en mois. Un taux de tentatives de 1 000 est une estimation grossière et arbitraire.

Tableau de Classe des Mots de Passe Capturés

(Durée de vie du mot de passe: 1 mois)

	Taille	**Espace**		**Probabilité**
Aléatoire, alphabétique minuscule	7	8.E+09		3
	9	5.E+12		2 095

	10	1.E+14		54,463
	11	4.E+15		1,416,028
	12	1.E+17		4.E+07
	14	6.E+19		2.5E+10
Aléatoire, alphanumérique	7	4.E+12		1,359
	8	2.E+14		84,236
	9	1.E+16		5,222,641
	14	1.E+25		4.8E+15
“fish ate blue house”	9	3.E+12		1,047
	10	7.E+13		27,231
	11	2.E+15		708,014

Remarquons que le protocole d'authentification LANMAN peut grandement compromettre l'espace des mots de passe. Ces tableaux supposent que ce danger ait été écarté. Voir “Mots de Passe LANMAN” dans *Mise en Réseau*.

Exemple de Stratégie A

Nous présentons maintenant la première des deux stratégies simples pour les mots de passe. Un site de Niveau 2 est dans une situation peu sûre au niveau du réseau et décide d'instaurer une politique agressive pour tous les mots de passe. Le site prend en considération les pires cas représentés par le tableau des Classes des Mots de passe capturés, ci-dessus, et requiert que la probabilité d'exposition soit de 1 pour 1000 ou moins et une durée de vie de mot de passe de trois mois. Ceci signifie que, par exemple, un utilisateur qui sélectionne un mot de passe aléatoire en caractères alphabétiques minuscules peut utiliser une longueur de 11. (Cette probabilité est de 2 832/3 ou seulement 944, mais assez proche de 1 000).Tout en reconnaissant que des mots de passe de cette longueur ne sont pas simples à conserver en mémoire, le site met en place un certain nombre de conseils concernant le stockage des document où l'on aurait écrit les mots de passe.

Exemple de Stratégie B

Dans cet exemple un réseau “sûre” décide que les mots de passe administratifs devraient être plus protégés que ceux des utilisateurs réguliers. Le site divise Tableau des Classes de Mots de passe - Tentatives d'ouverture de session (ci-dessus) en 3 classes de mots de passe basés sur cette probabilité:

Classe A 100 à 1 000
Classe B 1 000 à 100 000
Classe C 100 000 ou plus

Les probabilités en dessous de 100 sont considérées comme trop petites, et au-delà d'environ 1 000 000 comme excessivement larges. (Ainsi, les probabilités au delà de 1 000 000 présentent un risque de détermination de mot de passe considérablement moins important que d'autre niveaux de risques.)

Le site configure sa stratégie de compte et de mots de passe utilisateurs en accord avec les nécessités de la classe de mots de passe suivante. Ce tableau montre les nécessités de la classe

de mots de passe que le site devrait imposer qu'il soit au Niveau 1 ou 2. Les utilisateurs peuvent utiliser n'importe quel schéma de mots de passe qui correspond aux spécifications minimum. Remarquons que la résistance varie au sein d'un schéma et, toutes les autres considérations étant égales, les utilisateurs devraient choisir la pratique la plus solide au sein d'une classe donnée.

	Niveau 1	**Niveau 2**
Utilisateur Régulier	Classe A	Classe B
Administrateurs modérés [1]	Classe B	Classe C
Administrateurs & Opérateurs de Sauvegarde [2]	Classe B	Classe C

[1] Inclus les utilisateurs avec Pouvoir, et les opérateurs de Server, Comptes et impression.
[2] A l'exception du compte local Administrateur.

Ce site met la Durée de Verrouillage (non montré dans le tableau) égale au temps de remise à zéro du compteur, le minimum que la fenêtre permet.

Une brèche concernant l' Exposition des Mots de Passe sur le Réseau

Windows NT a été critiqué pour l'exposition des mots de passe sur le réseau. Windows NT ne crypte pas lui même le trafic réseau. Alors qu'il fournit une protection réseau modeste pour ses mots de passe, ses techniques sont vulnérables aux attaques modernes. Parce que les mots de passe de Windows NT sont susceptibles d'être attaqués par force brute, leur seule protection est leur espace. Si votre réseau est exposé à des éléments malveillants, et que vous ne pouvez pas assurer que vos utilisateurs vont sélectionner des mots de passe longs et aléatoires, vous devriez crypter *tout* le trafic réseau Windows NT. Ceci peut certainement résoudre les problèmes d'exposition de mots de passe. Et après tout, si votre réseau contient des éléments hostiles, ne voudriez vous pas protéger tout le trafic réseau par cryptage ? (Vous aurez besoin de produits fournis par des sociétés tierces. Voir *Mise en Réseau*.)

Mots de Passe pour le Compte Local Correspondant.

Un utilisateur qui travaille avec son compte “normal” peut avoir besoin d'un accès (par exemple, pour se connecteur sur un répertoire partagé) à un ordinateur distant dont la portée n'inclut pas son compte normal. Le cas le plus courant est celui où la ressource se situe dans un domaine différent sans une relation d'approbation correspondante. La façon la plus transparente pour s'accommoder de cela est de créer un compte local sur l'ordinateur distant avec le même nom de compte et mot de passe que celui de l'utilisateur régulier. (Voir “Domaines, Approbations & Portée des Comptes” *dans Domaines & Restrictions d'accès de Base*.)

L'on pourrait se demander s'il est prudent d'utiliser le même mot de passe pour à la fois le compte régulier et ce compte “correspondant”. Si le mot de passe est compromis sur le système distant, il peut être utilisé pour accéder à n'importe quel ordinateur sur lesquels le compte normal de l'utilisateur peut se connecter localement ou à distance. Considérez cela comme sûr sauf si l'ordinateur distant ne dispose pas de protections physiques adéquates et pose un risque de sécurité particulier , voir la section “Protection des Mots de passe cryptés & SYSKEY” dans *Stratégies Générales*.

Remarquons que si un utilisateur peut modifier son propre mot de passe, il doit maintenir la politique que vous avez mis en place. Vous pouvez bien évidemment l'empêcher de changer son mot de passe que ce soit pour son compte régulier ou son compte local correspondant.

Filtre de Mots de Passe

Les Administrateurs peuvent installer des programmes spéciaux qui refusent ou acceptent un nouveau mot de passe utilisateur à partir d'un certain nombre de règles définies. Ces programmes existent sous formes de DLL (bibliothèques de liaisons dynamiques). Microsoft fournit une telle DLL nommé “PASSFILT” qui requiert au moins 6 caractères avec des restriction sur ces derniers. Ces restrictions font que l'espace de mots de passe de PASSFILT (le nombre total de possibilités) inférieur à un schéma qui utiliserait des caractères choisis aléatoirement, et PASSFILT n'évite pas l'utilisation de mots de passe aussi simples que “Frog00.” Ce guide ne recommande pas (et ne dissuade pas) d'utiliser PASSFILT parce qu'il impose aux utilisateurs consciencieux (qui choisiraient autrement des mots de passe aléatoire) d'utiliser des mots de passe sensiblement plus longs pour obtenir la même protection et n'évite pas les mots de passe simplistes. De cette façon, PASSFILT entraîne à croire que limiter les caractères du mot de passe accroît leur résistance, alors qu'en réalité il fait le contraire.

Vous devez activer ces DLL en ajoutant leur nom (sans le suffixe “.DLL”) à la valeur multi-chaîne nommée “Notification Packages” dans la clé de Registre:

```
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa
```

qui définit toutes les DLL de ce type. Mettez-les dans la racine système et assurez-vous que seuls les administrateurs et l'utilisateur SYSTEM puissent les modifier ou les remplacer. Remarquons que la DLL reçoit le mot de passe non crypté de l'utilisateur et doit le gérer prudemment pour éviter toute exposition accidentelle.

Le sujet “Notification Packages” est aussi traité dans “La fonction de Notification du Mot de passe ” dans *Stratégies Générales*.

Résumé

En résumé, il y a trois composantes pour protéger les mots de passe de Windows NT :

- Les attaques au travers des mécanismes normaux d'authentification peuvent effectivement être contournés par des complexités de mots de passe raisonnables et le verrouillage de comptes.
- Les attaques dirigées contre les Mots de passe cryptés stockés dans la base SAM (ou des copies). Il y a des façons efficaces de combattre cela. Voir “Protection des Mots de passe cryptés & SYSKEY” dans *Stratégies Générales*.
- Les attaques qui écoutent les mécanismes d'authentification de Windows NT. Votre protection la plus complète est de rechercher des logiciels capables de crypter le trafic réseau de Windows NT. Voir *Mise en Réseau*.

Les stratégies de mots de passe ne représentent pas une science précise, et il y a de nombreuses façons d'améliorer nos conseils par rapport à votre site et vos utilisateurs. Une considération essentielle est que les mots de passe longs, complexes sont difficiles à déterminer mais sont plus susceptibles d’être écrits ce qui est une exposition supplémentaire. La complexité des mots de passe constitue toujours un certain compromis.

Si vous avez besoin de probabilités plus élevées dans le Tableau des Classes de Mots de passe - Tentatives d'ouverture de session, nous vous recommandons d'augmenter le délai de réinitialisation du verrouillage plutôt que d'imposer à vos utilisateurs de se rappeler de longs mots de passe.

Exiger qu'un utilisateur sélectionne son premier mot de passe à “la première ouverture de session” n'est pas un contrôle de sécurité solide. Les utilisateurs consciencieux le feront

correctement mais ceux qui sont plus négligents choisiront des mots de passe faibles quoi que vous fassiez. Un mot de passe utilisateur n'est pas une protection contre des Administrateurs "Pleins Pouvoirs" et des Opérateurs de Compte. Cependant, vous pouvez utiliser cette fonction pour forcer les utilisateurs à modifier leur mot de passe si vous suspectez qu'il a été compromis.

Certains schémas de mots de passe limitent l'espace (le nombre total de combinaisons) en restreignant les caractères du mot de passe, par exemple, en requérant deux chiffres (0-9) dans le mot de passe. Ceux-ci pénalisent modestement les utilisateurs consciencieux en leur faisant choisir de longs mots de passe pour atteindre un espace équivalent. Par exemple, une stratégie qui requiert deux majuscules, deux minuscules, et deux chiffres est satisfaite par “AAaa00” – difficilement un mot de passe résistant. Cependant, ces schémas peuvent faire comprendre à l'utilisateur moyen l'importance du choix d'un mot de passe. Le fait d'utiliser de telles techniques est très subjectif mais vous devriez calculer la réduction de l'espace des mots de passe avant de prendre votre décision.

Sections Associées:

“Protection des Mots de passe cryptés & SYSKEY” dans *Stratégies Générales*

Références:

[Sutt96] “Choix des Mots de Passe” dans le Chapitre 3, *Votre Environnement de Travail*, p. 47.

[Sutt96] “Comptes” dans le Chapitre 7, *Gestion des Groupes et des Comptes*, p. 161. En particulier le sujet “La Stratégie de Compte,” p. 168, et “Vos Mots de Passe,” p. 172.

11. Fichiers de Stratégie Système

Consultez votre documentation système, les Notes ci dessous, et le chapitre 10, *Editeur de Stratégie Système*, dans [Sutt96] pour une description globale des stratégies système. La configuration de la Stratégie Systèmes est un processus exigeant et vous devez consulter les références soigneusement.

Ces conseils recommandent une politique de fichiers de stratégie simple basée sur le domaine au Niveau 2. Vous pouvez évidemment étendre ce simple schéma, mais ces recommandations ne le prescrivent pas. (Voir " Forcer l'Utilisation des Fichiers de Stratégie " ci dessous.) Les deux modes de base pour utiliser le fichier stratégie sont appelés "Mise à jour Automatique " et "Mise à jour Manuelle." (La section " Mode Automatique contre Mise à jour Manuelle" ci-dessous décrit les critères pour choisir entre les deux.)

Conseils

Niveaux 1 & 2:

Ces conseils *recommandent* d'installer un fichier de Stratégie Système avec la configuration suivante. Beaucoup de ces Stratégie Système représentent des contrôles de sécurité modestes dans la plupart des environnements.

- Si vous choisissez d'utiliser le mode Mise à jour Automatique, créez et installez un fichier NTCONFIG.POL dans le partage NETLOGON sur chaque contrôleurs de domaine avec la configuration ci dessous. Pour la Mise à jour Manuelle créez et installez le fichier à l'endroit choisi.
- Se référer à la section "Stratégie Utilisateur Recommandée par Défaut pour des Utilisateurs non Administrateurs ," qui suit. Mettez en place les stratégies marquées "✔." Celles marquées avec un "**?**" nécessitent de plus amples considérations mais ne sont pas prescrites par ce guide (bien que d'autres pourraient). Le guide recommande à la place celles marquées "**X**."
- Les fichiers Stratégie devraient appartenir à des Administrateurs avec l'ACL suivante:

Tout le monde	Lire
Administrateurs	Contrôle total
SYSTEM	Contrôle total

- A moins que votre site ne nécessite autre chose, le mode Mise à jour Automatique assure que la même configuration des stratégies sera définie dans chaque famille de domaine. (Voir "Mode Automatique contre Mode de Mise à jour Manuel," plus bas).
- Confirmez le fait que la stratégie de "Mise à jour distante" est configurée dans chaque base de Registres des ordinateurs. Elle est en Mode de Mise à jour Automatique après l'installation. Utilisez l'Editeur de Stratégie Système pour configurer la Stratégie "Mise à jour distante", ou n'importe quel éditeur de base de Registres sur la clé:

  ```
  HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Update
  ```

  En mettant sa valeur "UpdateMode" à:

UpdateMode: REG_DWORD: 0x1	pour la Mise à jour Automatique
UpdateMode: REG_DWORD: 0x0	pour la Mise à jour Manuelle

Examen Régulier:

- Assurez-vous que les fichiers de Stratégie reflètent bien la politique actuelle du site.

- ❑ Assurez-vous que les Stratégies soient mises en place totalement pour la portée désirée. (En particulier, que “Mise à jour distante” soit activée sur chaque ordinateur.)
- ❑ Assurez-vous que le partage NETLOGON et que ses fichiers Stratégie sur les contrôleurs de domaine soient correctement protégés contre l’accès publique.
- ❑ Justifiez les cas où les Stratégies ordinateur dans différents domaines ne définissent pas le même jeu de stratégies.

Notes

Stratégie Utilisateur Recommandée par Défaut pour des Utilisateurs non Administrateurs

Affichage

Restreindre le Panneau de Contrôle “Affichage”

? Cacher la page de l'écran de veille

C’est une manière utile d'empêcher les utilisateurs de modifier un économiseur d’écran verrouillage pré-installé. Toutefois, cela ne protège pas les entrées de la Base de Registres qui définissent l’économiseur d’écran lui même. Donc, cacher ce panneau n’empêche pas un utilisateur de modifier son économiseur d'écran en utilisant d’autres outils ou en éditant directement la base de registres.

Shell

Restrictions

? Retirer la commande Exécuter

Il y a de nombreuses façons pour des utilisateurs de lancer des commandes arbitraires, enlever ceci n’aurait pas de sens. La commande Exécuter peut être utile contre certaines formes de spoofing et la laisser dans le Menu Démarrer encourage les gens à s’en servir. (Voir Le Problème du “.”dans *Spoofing*.) A moins que vous n’empêchiez toutes les autres façons d'exécuter des commandes (ce qui est invraisemblable), il y a peu de façon d'imposer cette stratégie.

✔ Désactiver la Commande Arrêter

Assurez-vous que la mise hors-service se fait en utilisant la fenêtre sécurité (“chemin de confiance”) – une alternative plus sûre.

Shell Windows NT

Restrictions

✔ Utiliser seulement les extensions shell approuvées

Cette stratégie réduit les attaques de spoofing potentielles et est particulièrement importante pour les administrateurs.

Système

Restrictions

✔ Désactiver les outils d'édition du Registre

Bien que cela empêche l’utilisation d’outils spécifiques, cela n'empêche pas d’accéder à la Base de registres en utilisant d’autres programmes. Bien que ce soit prudent dans certains cas, cela fournit peu de protection contre une attaque déterminée. Voir “Activer les Editeurs de Registre” dans *Stratégies Générales*.

? Exécuter seulement les Programmes Autorisés

Facilement contourné. Voir “Restrictions d'Applications Utilisateur” ci dessous.

Stratégies Recommandées par défaut

Réseau

System policies update (mise à jour des fichiers de Stratégie)

✔ Mise à jour distante

Configurez le mode Automatique ou Manuel en conformité avec votre stratégie. Choisissez Afficher les Messages d'Erreurs, qui imprime un message pendant la connexion si le fichier stratégie n'est pas disponible sur le réseau. Il y a en fait rarement besoin de définir cette stratégie car elle doit être correctement configurée sur un ordinateur avant que cet ordinateur ne puisse charger un fichier de Stratégie.

Réseau Windows

Partage

? Créez des partages cachés (station de travail)

? Créez des partages cachés (serveur)

Voir "Partages Administratif Cachés " dans *Partages Réseaux*.

Système Windows NT

✔ Bannière d'ouverture de session (Logon Banner)

Présente une fenêtre pendant la connexion de l'utilisateur que vous pouvez utiliser d'une ou deux façons selon la stratégie de votre site: (1) un avertissement officiel ("un message officiel") à propos de la politique concernant l'utilisation de cet ordinateur, ou (2) une note de sécurité aux utilisateurs sur laquelle ils peuvent compter. Configurez l' "Intitulé," le titre de la fenêtre, et le "Texte," le texte affiché dans la fenêtre. En tant qu'élément de sécurité, la première utilisation peut servir comme un moyen de découragement mineur contre des intrus potentiels. En outre, la plupart des sites considèrent cela comme une preuve dans les recours légaux en cas d'utilisation non autorisée.

Accès Distant Windows NT

X Nombre maximum de tentatives d'authentification

X Temps maximum pour l'authentification

X Déconnexion automatique

Voir *Service d'Accès Distant*. Leur configuration fait partie intégrante de l'installation de RAS sur un ordinateur et ne les modifiez plus une fois installé. Elles ont un impact mineur sur la sécurité.

Vous désirerez peut-être configurer certaines des stratégies non cochées mais seulement pour certains utilisateurs. Par exemple, "Désactiver les Outils d'édition du Registre" peut être mis pour tout le monde à part les administrateurs. Vous voudrez peut-être installer certains "papiers peints" (écran de fond) pour les administrateurs. Ceci nécessite de créer un groupe stratégie système pour les administrateurs pour qu'ils puissent être traités à part. (Notez que de nombreuses stratégies système, comme la configuration de papier peint, ne sont pas forcées et l'utilisateur peut librement les modifier une fois connecté. Voir "Stratégies Utilisateurs Protégés " plus bas.) Voir les références générales, ci-dessous.

Forcer l'Utilisation des Fichiers de Stratégie

Toutes les stratégies “ordinateurs” peuvent être mises en place (pour un ordinateur donné) indépendamment du compte sur lequel on est connecté en les configurant dans la base de Registres à l'aide d'un éditeur de base de registres ou un programme administratif spécifique. La seule raison impérative pour définir ceci est lorsque ces stratégies doivent être différentes de celles des comptes sur lesquels on se connecte. Par ailleurs, cela peut être plus facile de définir des stratégies ordinateurs en utilisant un fichier de stratégie parce que celles-ci sont automatiquement activées à chaque connexion de l’utilisateur. Ainsi, quand vous modifiez la stratégie ordinateur dans un fichier stratégie, il se propagera plus ou moins vite à tous les ordinateurs au fur et à mesure que les utilisateurs se connectent.

Les stratégies “Utilisateur” peuvent aussi être imposées sans fichier de stratégie pour celles qui s'appliquent à tous les utilisateurs. Toutefois, elles sont difficiles à appliquer sans fichiers de stratégie parce que les stratégies utilisateurs résident dans le profil utilisateur, qui est plus difficile à modifier pour l’administrateur. Quand différentes stratégies sont à appliquer à différents utilisateurs, le fichier de stratégie est l’option la plus pratique.

Mode Automatique contre Mise à jour Manuelle

Dans le **Mode Mise à jour Automatique** (comme configuré dans la stratégie de Mode de Mise à Jour), les stratégies utilisateurs et ordinateurs sont prises sur le contrôleur de domaine du compte de l’utilisateur. Ceci veut dire que différentes stratégies ordinateurs peuvent s’appliquer à différents utilisateurs sur le même ordinateur. Alors qu'ils n'ont pas totalement tort, les administrateurs débutants dans les fichiers stratégies peuvent penser que la même stratégie système s’applique toujours à un ordinateur donné. Aussi, les connexions aux comptes locaux ne sont pas sujet aux fichiers stratégie en Mode de Mise à jour Automatique.

Si c’est important que la même stratégie ordinateur et utilisateurs s’applique à *tous* les utilisateurs sur un ordinateur donné, indifféremment de leurs comptes de domaine, vous pouvez utiliser le **Mode de Mise à jour Manuelle** (comme configuré dans la stratégie) sur cet ordinateur. Dans le Mode de Mise à jour Manuelle, vous spécifiez un endroit pour le fichier stratégie, que ce soit sur l’ordinateur lui même ou un répertoire réseau partagé. (Le partage NETLOGON sur le contrôleur de domaine est un endroit pratique.) Le Mode de Mise à jour Manuelle applique les stratégies à toutes les connexions, y compris aux comptes locaux. Aucun des modes Manuels ou Automatique n'est de façon inhérente moins sécurisé que l’autre, mais l'un sera plus approprié que l’autre sur un ordinateur donné.

Restrictions d'Applications Utilisateurs

La stratégie appelée “Ne lancer que des Applications Windows autorisées” laisse l’administrateur définir un jeu d’applications (comme “EXPLORER.EXE” ou “WINWORD.EXE”) qui sont les seuls qu'un utilisateur, pour qui les stratégies s’appliquent, peut exécuter. (Même Explorer doit être sur la liste avant d’être exécuté.) Cela les empêche aussi d être exécutés comme Applications au démarrage et à partir de la fenêtre Sécurité du Gestionnaire de tâche Windows. Toutefois, il y a plusieurs précautions:

- Beaucoup d’applications ont des fonctions “exécuter” qui permettent aux utilisateurs de lancer d’autres programmes à partir de l’application. Ces applications habituellement n'appliquent pas ces restrictions. En particulier, la fenêtre de commandes DOS ne renforce pas cette liste. Toutefois, vous pouvez empêcher les utilisateurs d'exécuter des applications avec l’option exécuter en les enlevant de la liste (comme CMD.EXE pour la fenêtre de commandes DOS).

- Si un utilisateur peut lire un fichier exécutable, non autorisé, il peu en faire une copie dans un autre répertoire et renommer le fichier avec un nom autorisé et l'exécuter sous le nouveau nom. Vous pouvez empêcher cela en enlevant la permission “R” de ces fichiers, en laissant le “X.” (Voir “Retirer le ‘R’ des fichiers programmes” dans *Spoofing*.)
- Un utilisateur peut importer n’importe quel programme sur le système (plus notablement un qui le laisse exécuter d’autres programmes de son choix), nommer le programme avec un nom autorisé, et après l'exécuter.

En tant que contrôle de sécurité, cette méthode est faible et nos recommandations ne prescrivent donc pas son utilisation. Mettre des ACLs sur les fichiers programmes est bien plus efficace. Toutefois, vous trouverez peut-être cela utile pour “décourager” les utilisateurs d'exécuter des programmes qu’ils ne devraient pas.

Notez que les pouvoirs d’un utilisateur viennent de son compte et de sa session– pas des programmes qu’il exécute. Par exemple, empêcher un utilisateur d’utiliser l’éditeur de la base de registres ne l'empêche pas d’accéder à la Base de Registres– cela veut juste dire qu’il doit utiliser un autre programme, peut-être un qu’il aurait crée.

Stratégies Utilisateurs Protégés

La clé de la Base de Registres:

```
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Polic
ies
```

est en lecture-seule pour l’utilisateur actuel. Les stratégies mises en places par des éléments dans cette clé sont les seules que les utilisateurs ne peuvent modifier eux mêmes.[21] Toutes les stratégies recommandées dans “Stratégie Utilisateur Recommandée par Défaut pour des Utilisateurs non Administrateurs,” plus haut, sont dans cette clé.

Stratégies personnalisées.

On peut ajouter des stratégies à l’éditeur de Stratégie Système et ses fichiers en créant des fichiers standard *.ADM. Nous ne connaissons pas de documentation qui décrive leur format, bien que vous puissiez apprendre en étudiant les fichiers installés. Vous devez les installer dans l’éditeur de Stratégie Systèmes en tant qu'options de Modèles de Stratégie (Policy Template).

Références:

[Sutt96] La section “Editeur de Stratégie Système” dans le Chapitre 10, *Sous-systèmes et autres Caractéristiques de Sécurité*, p. 261.

[ConPln] Section “Stratégie Système” dans le Chapitre 3, *Gestion de l'Environnement de Travail Utilisateur.*

[21] Cependant, cette portion du Registre peut être chargé à partir des fichiers *.DAT dans le répertoire profile utilisateur sous WINNT pour lequel l'utilisateur peut avoir l'accès en écriture et potentiellement modifier. (Ceci est un peu compliqué parce que le système garde les fichiers *.DAT de l'utilisateur en question ouverts en accès exclusif, donc un utilisateur doit le modifier lorsqu'il est loggué à partir d'un autre compte.) Soulignons que les Stratégies de Sécurité (à partir des fichiers de Stratégie de Sécurité) sont écrits après le chargement du profile de l'utilisateur, et ses stratégies seraient susceptibles d'écraser des modifications éventuels par l'utilisateur.

12. Droits des Utilisateurs

Chaque ordinateur Windows NT possède une “Stratégie de Droits” locale qui associe les divers groupes et comptes utilisables sur cet ordinateur avec environ 30 Droits. Les Droits ne sont pas une propriété de l'utilisateur ou du groupe, et un compte peut avoir différents droits sur différents ordinateurs. Les Administrateurs "Pleins Pouvoirs" gèrent les Droits d'un ordinateur en utilisant le Gestionnaire des Utilisateurs.

Quand Windows NT crée un session locale (primaire) ou distante (secondaire), il attache les Droits associés avec le compte utilisateur et tous les groupes de l'utilisateur à la session. Ces Droits sont hérités par les programmes qui fonctionnent au sein de cette session et à beaucoup de serveurs à partir desquels ces programmes exigent des services. Les Droits permettent aux programmes des capacités particulières. Les Droits d'ouverture de session ne sont pas affectés par les modification aux Droits pendant la durée de vie de la session. Ensemble, une identification de compte utilisateur, les appartenances aux groupes, et les Droits déterminent les pouvoirs sur le système.

Les Droits Systèmes par défaut sont sensiblement sécurisés et les conseils ci-dessous ne prescrivent que peu de modifications. La plupart des Droits ne présentent d'intérêt que pour le système d'exploitation lui même et ne sont assignés qu'à peu de comptes.

Conseils

Niveaux 1 & 2:

Les Droits par Défaut sont déjà sensiblement sécurisés et nous ne proposons que peu de modifications.

- Nous *recommandons* que vous remplaciez “Tout le Monde” (si il existe) par “Utilisateurs” dans le Droit d' “**Ouvrir une sessions localement**” et **“Accéder à cet ordinateur à partir du réseau**.” Votre Stratégie peut aussi imposer de pousser davantage les restrictions de ces Droits comme décrit dans “Droits de connexion dans des environnements à plusieurs domaines” dans *Domaines & Restrictions d'Accès de Base*. Tout le Monde et Utilisateurs concernent en général les même comptes. Cependant, permettre à Tout le Monde d'ouvrir une session locale ou distante semble trop large en principe général. Remarquons que ceci n'inclut pas l'accès distant par le compte Invité parce que par défaut, il n'est pas un membre de Utilisateurs.
- Retirez tous les utilisateurs et groupes du Droit nommé “**Outrepasser le Contrôle de Parcours**.” Il n'y a rien de dangereux concernant l'assignation aux utilisateurs du Droit d' “Outrepasser le Contrôle de Parcours,” tant que tous les utilisateurs système comprennent que restreindre l'ACL d'un répertoire à d'autre utilisateurs n'interdit pas nécessairement l'accès à ses fichiers et sous-répertoires. En prenant l'idée que les utilisateurs tendent à penser le contraire, et qu'Outrepasser le Contrôle de Parcours peut être nécessaire,[22] le guide recommande que vous ne l'assigniez à personne. Vous pouvez mettre ce Droit sans danger aux utilisateurs administrateurs qui ont un large accès de toute façon.

[22] Il y' a au moins un rapport mentionnant que le fait de retirer ce Droit ce certains comptes peut entraîner un crash du système d'exploitation (le fameux “blue screen of death”). Nous ne pouvons pas confirmer cela pour le moment.

- Nous vous *recommandons* d'ajouter les Opérateurs de Serveur et Utilisateurs avec Pouvoirs au Droit d' "**Augmenter la priorité de planification**." C'est un privilège bénin en terme de sécurité et le donner plus largement aide à réduire l'utilisation de compte administrateurs 'Plein Pouvoirs'.
- Retirez le Droits "**sauvegarde**" et "**restauration**" aux Opérateurs de Serveur. Ces Droits extrêmement critiques conviennent davantage aux comptes utilisés pour faire *seulement* des sauvegardes et des restaurations de données, normalement les Opérateurs de Sauvegarde.

A l'exception des descriptions fournies par ces indications, n'étendez pas l'allocation des Droits à moins que vous ne conceviez pleinement toutes les ramifications. Beaucoup de Droits permettent en effet aux utilisateurs un accès illimité au système.

Notes

Droits Communs

La section suivante résume plusieurs Droits mentionnés dans le Guide:

Ouvrir une session localement
Accéder à cet ordinateur depuis le réseau

Un compte doit avoir le Droit d'"ouvrir une session localement" avant que le système ne lui autorise la connexion locale (primaire), et d'"accéder à cet ordinateur depuis le réseau" avant que le système ne crée une session distante (secondaire) pour ce compte. Ces deux droits sont une façon effective de contrôler qui peut utiliser quel ordinateur.

Remarquons que des services fournis par des sociétés tierces peuvent ne pas se baser sur les mécanismes d'authentification distantes natifs de Windows NT, et peuvent fournir des fonctions aux utilisateurs distants qui n'ont pas le droit d'accéder à l'ordinateur via le réseau. Il faudrait alors espérer qu'un tel service possède un contrôle utilisateur assez solide. Gérez ce genre de service au cas par cas.

Sauvegarder les fichiers et répertoires
Restaurer les fichiers et répertoires

Ceux-ci sont probablement les Droits les plus puissants et permettent d'outrepasser les ACLs pour lire et écrire. Avec les outils standard de Windows NT, il est difficile pour les programmes qui possèdent ces privilèges de lire ou de modifier directement des fichiers que leurs ACLS refuseraient, mais créer des programmes spéciaux pour effectuer cette mission est à la portée d'un grand nombre d'administrateurs et d'agresseurs.

Prendre possession des fichiers et dossiers

Ce puissant Droit permet à un compte de devenir le propriétaire de l'objet d'un autre utilisateur (comme les fichiers, répertoires et clés de Registre). En tant que propriétaire, vous pouvez modifier l'ACL pour vous octroyer un accès illimité. Cependant, ce Droit ne vous permet pas d'inverser l'appartenance en remettant l'appartenance sur le propriétaire précédent.

Debugger des programmes

Ce Droit permet à un utilisateur d'intervenir dans le fonctionnement des programmes lancés par un autre utilisateur. C'est un privilège critique puisque l'autre utilisateur peut très bien être un Administrateur, ce qui permet à un debugger malin d'obtenir les capacités de l'administrateur.

Outrepasser le Contrôle de Parcours

Suspendre la vérification d'ACL que le système effectue lorsqu'un programme utilise un répertoire dans un nom de chemin. Sans ce Droit, si vous n'avez pas la permission nécessaire pour entrer dans un répertoire, vous n'obtiendrez jamais d'accès à quelque objet que ce soit au sein de l'arborescence en question, même si vous avez accès à cet objet. Par analogie, si la porte d'un bâtiment est fermée, vous ne pourrez pas atteindre un bureau même si sa porte est ouverte. Tout ceci change lorsque vous donnez à un utilisateur le droit d'Outrepasser le Contrôle de Parcours. Alors que vous ne pouvez toujours pas Lire ou Ecrire dans le dossier vous pouvez passer au travers en désignant un objet dans l'arborescence pour lequel vous avec un accès (pourvu que vous connaissiez son chemin). Par défaut, Tout le Monde possède ce Droit.

Arrêter le système

Ces conseils ne considèrent pas le fait d'arrêter le système (un “dénie de service”) comme un problème de sécurité, bien que cela soit un important problème opérationnel. Voir aussi “Arrêter le Système” dans *Stratégie Générale*.

Chapitres et Sections associés:

Domaines & Restrictions d'Accès de Base, Droit d'ouvrir une session localement et à distance

Services Systèmes, Droits qui s'appliquent au compte SYSTEM.

Comptes Utilisateurs & Groupes, Droit d'ouvrir une session localement contre le paramètre “Se connecter à” dans un compte.

Références:

[Sutt96] “Droits des Utilisateurs” dans le Chapitre 7, *Gérer les Groupes et les Comptes*, p. 182.

[NetGd] “ Droits des Utilisateurs ” dans le Chapitre 2, *Sécurité Réseau et Planification de Domaine*.

13. Stratégie d'Audit et Journal Sécurité

Windows NT peut enregistrer un nombre important d'événements liés à la sécurité dans son journal sécurité, chacun avec un certain nombre de détails. Cependant, beaucoup d'enregistrements d'audit manquent d'informations essentielles, et beaucoup d'autres ne contiennent aucune information analysable manuellement. L'analyse d'audit de Windows NT est limitée à un visualiseur convivial mais simpliste. Windows NT supporte entièrement les outils d'analyse fournis par des sociétés tierces, et vu l'importance des informations que peut générer la journalisation, l'audit semble limité sans ce genre d'outils. Reportez-vous aux références à la fin de ce chapitre pour un aperçu général des possibilités de journalisation sécurité (audit) de Windows NT.

Conseils

Niveaux 1 & 2:

L'intention de ces directives n'est pas de limiter la quantité ou le type de données que les administrateurs de site choisissent d'enregistrer. Cependant, la philosophie du Guide étant d'inclure uniquement les procédures pratiques de sécurité, elles incluent l'audit minimal. La difficulté dans la prescription de n'importe quel niveau d'audit est que ce dernier dépend totalement du temps et de l'énergie que les administrateurs sont disposés à investir dans sa maintenance.

☞ Par conséquent, considérez ces directives pour l'audit comme un " point de départ recommandé".

Dans la table qui suit les "Serveurs importants " sont des ordinateurs équipés de Windows NT qui exécutent des fonctions de partage de groupe de domaine importantes, qu'ils soient ou non contrôleur de domaine. Les "Workstation" sont tous des ordinateurs qui ne sont ni des "Serveurs importants", ni des contrôleurs de domaine. (Le terme de "contrôleur de domaine" inclue les contrôleurs du domaine secondaires, auxquels la stratégie d'audit est répliquée automatiquement.)

- Configurez les Stratégies de l'Audit qui utilisent le Gestionnaire des Utilisateurs d'après le tableau des événements de l'audit, ci-dessous.
- En utilisant l'Observateur d'Evénements, paramétrez le journal de sécurité comme ceci:
  - La zone "taille maximale du journal" doit contenir la quantité d'espace disque que vous souhaitez dédier à la sauvegarde des traces de l'audit. Cela influe directement sur la fréquence à laquelle vous sauvegardez le journal sur unité de sauvegarde. Il n'existe pas de valeurs particulières, bien que nous vous recommandions d'y consacrer au moins 10 Mo, valeur soumise à expérimentation.
  - Mettez le "bouclage du journal des événements" sur "Ecraser les événements si nécessaire". (Voir le raisonnement suivant.)
- Contrôlez régulièrement la taille du journal de l'audit, sauvegardez-le sur un support de "longue durée" (comme une bande magnétique), puis effacez-le.
- **Optionnel**: Créez une partition logique sur le disque réservé pour le journal de sécurité. Placez le fichier du journal sur ce disque (Voir “Autres emplacements possibles pour le journal de sécurité,” plus loin), et affectez à la "taille maximale du journal" la valeur de l'espace disque réservée au journal de sécurité sur cette unité logique. Cela permet de

s'assurer que le journal atteindra sa taille maximale spécifiée sans en être limité par l'espace disque. (Vous pouvez aussi préciser une taille fixée sur ce disque.)

Examen Régulier:

- Assurez vous que les journaux de sécurité sauvés sont stockés de façon sûre et accessibles en cas de besoin.

Tableau des événements d'audit

	Workstations	**Serveurs Importants & Contrôleurs de Domaine**
Ouverture et fermeture de session	Niveaux 1 & 2	1 & 2
Démarrage, Arrêt & Système [1]	1 & 2	1 & 2
Modification de Stratégie Sécurité[1]	1 & 2	1 & 2
Gestion des Utilisateurs & Groupes [1]	1 & 2	1 & 2
Utilisation des Droits des Utilisateurs [2]	—	—
Accès aux Objets & Fichiers [2] [3]	—	—
Suivi de Processus [2]	—	—

[1] Ce sont des événements généralement rares en dehors des contrôleurs de domaine, ce qui les rend d'autant plus "sauvegardables". Ils sont optionnels au Niveau 1.

[2] Ces catégories produisent beaucoup d'événements peu utiles sans outils d'analyse.

[3] Le Guide ne conseille généralement pas d'audit d'objets. Cependant, il peut être approprié pour les deux Niveaux au cas par cas.

Notes

Ces notes incluent quelques-uns des aspects les moins connus du journal de sécurité de Windows NT. Le Guide ne prescrit pas l'usage de ces caractéristiques, bien que certaines politiques de site puissent les exiger.

L'Audit d'Objet enregistre toujours les Objets SAMs

Si vous activez "Accès fichier et objet" dans la stratégie d'audit, la plupart des accès de bas niveau à la base de donnée des comptes utilisateurs du Registre (la "SAM") seront audités comme des événements d'accès objet, bien que l'information de contrôle de l'audit ne soit pas assignée explicitement à ces clés du Registre. Comme la plupart des accès objet, le journal de sécurité n'enregistre que les autorisations d'accès demandées par le programme lorsqu'il ouvre les clés, et ces permissions sont souvent bien plus larges que ce que le programme utilise réellement. D'où, sans des outils d'analyse de l'audit plus sophistiqués, les informations que vous pourrez glaner seront limitées. Ces Conseils ne prescrivent pas de vérifier ces objets. Voir [KBase] Q149401.

Droits non audités

La stratégie d'audit "Utilisation des droits de l'utilisateur" ignore systématiquement l'utilisation des droits suivants: "Outrepasser le contrôle de parcours", "Générer des audits de

sécurité", "Créer un objet-jeton", "Déboguer des programmes" et "Remplacer un jeton niveau de processus".

L'audit n'enregistre pas non plus l'utilisation des deux droits de sauvegarde et de restauration des fichiers et des répertoires à moins que la clef du Registre:

```
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Lsa
```

ait une valeur de type REG_DWORD nommée " FullPrivilegeAuditing " dont la valeur serait 1. Enregistrer ces événements inondera probablement le journal de sécurité avec des informations accessoires. Notre Guide ne prescrit pas l'audit de l'utilisation de ces droits.

Auditer les "Objets de Base (Base Objects)"

"Les Objets de Base" sont des objets internes à Windows qui ne sont pas dans le système de fichier ou le Registre. Les utilisateurs ne voient pas et ne manipulent pas directement les "Objets de Base" bien que leurs programmes puissent y accéder. Windows NT n'audite pas l'accès à ces objets à moins que la clef du Registre:

```
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa
```

aie une valeur de type REG_DWORD nommé "AuditBaseObjects" dont la valeur est 1. (Sa valeur est 0 par défaut.) Le type d'audit "Accès fichier et objet" contrôle l'ensemble des émissions de ces événements. Les événements d'accès d'objet pour les Objets de Base sont identiques à ceux de l'accès au système de fichiers, mais ont un nom d'objet et des noms de permissions différents. L'audit de ces événements a tendance à inonder le journal de sécurité avec des événements de sécurité d'importance mineure aux yeux de la plupart des administrateurs. Notre Guide ne prescrit pas l'audit pour les Objets de Base. Voir aussi "ProtectionMode" dans Stratégies Générales.

Crash lorsque le Journal Sécurité est plein

Si la clef du Registre:

```
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa
```

possède une valeur de type REG_DWORD nommé "CrashOnAuditFail " dont la valeur est 1, le système d'exploitation s'arrêtera lorsque le journal de sécurité aura atteint sa taille maximale spécifiée, et l'option "Ne pas écraser les événements" sera sélectionnée automatiquement dans les paramètres du journal des événements de sécurité.(Cela réinitialise CrashOnAuditFail à 0 permettant ainsi à un administrateur de relancer le système et de corriger le problème d'espace disque).

Certains sites requiert que le système s'arrête s'il n'a plus les ressources nécessaires pour stocker les événements d'audit. Cela arrive lorsque le journal atteint sa taille maximale spécifiée, ou lorsque que le disque sur lequel est stocké le journal est plein. Ce guide ne prescrit pas cette action drastique même au Niveau 2. Les administrateurs devraient plutôt contrôler la taille du journal et l'empêcher de se remplir.

Autres emplacements possibles pour le journal de sécurité

La clé du Registre:

```
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\
     EventLog\Security
```

possède une valeur nommé "File" contenant le chemin et le nom du fichier journal de sécurité. Vous pouvez modifier l'emplacement du fichier (la modification prendra effet

lorsque le système aura redémarré). Vous pouvez utiliser ceci pour placer le journal de sécurité sur un volume dédié aux informations du journal de sécurité (peut-être avec d'autres informations dont la taille ne varie pas afin que vous puissiez garantir un certain espace disque consacré au journal de sécurité. Notez que les fichiers du journal de sécurité (dont l'extension est ".EVT") ne devrait pas être accessibles publiquement. Cependant, le système d'audit ouvre ce fichier exclusivement lors du démarrage du système, ce qui empêche l'accès public, même si l'ACL du fichier autorise un tel accès.

Droit de Gérer le Journal d'Audit

Le droit de "Gérer le journal d'audit et de sécurité" permet à un compte de visualiser et d'effacer le journal de sécurité, de sauvegarder le journal dans un fichier, et de positionner des informations d'audit sur des objets (comme les fichiers ou les clés du Registre). Il n'autorise pas la modification des paramètres du journal des événements (comme le "Bouclage du journal des événements") ou la gestion de la "Stratégie d'audit" à travers le "Gestionnaire des utilisateurs". Il s'agit d'un Droit sensible, bien protégé par défaut.

Audit d'Objets

L'audit par Objet (placer des informations d'audits, des SACLs, sur un objet tel qu'un fichier ou un répertoire) est un problème ouvert à débat qui ne peut être résolut que par les pratiques et stratégies de site. L'audit d'Objets n'est pas un substitut pour les contrôles des ACLs, et ces événements peuvent facilement submerger le journal de sécurité. Ils sont plus effectivement mieux utilisés avec des analyseurs d'enregistrement d'audit, et aucun n'est fournit avec Windows NT. Bien que nos conseils ne prescrivent pas l'audit d'objets, ils ne s'opposent pas non plus à son utilisation.

Références:

[Sutt96] Chapitre 8, *Audit Sécurité*, p. 193-199.

[RKitW] “Auditer les Evénements de Sécurité” dans le Chapitre 6, *Windows NT Security*. Quelques brèves informations à propos du journal sécurité.

14. Services Systèmes

Les services Windows NT sont des programmes que le système lance au démarrage. Les services continuent généralement de tourner en tâche de fond, répondant aux différentes requêtes des programmes que lance l'utilisateur ainsi qu'aux requêtes du réseau. Les administrateurs gèrent les services au travers de l'icône services du panneau de configuration.[23] Chaque service fonctionne à partir d'un compte spécifié dans Services du panneau de configuration, il s'agit généralement du tout puissant compte intégré SYSTEM. Les Services assument généralement l'identité des programmes qui appellent leurs fonctions en utilisant un processus appelé "personnification." Les Services peuvent alors gagner les capacités du demandeur (souvent appelé le "client") qui peuvent aller au delà des propres possibilités du compte inhérent au service.

Les logiciels que vous installez peuvent comporter des services, bien que cela requiert que l'installateur ait les pleins pouvoirs administratifs. Même au Niveau 1, vous pourriez vouloir mettre en place des pratiques du Niveau 2.

Conseils

Réduire les Services & leurs Capacités

Niveaux 1 & 2:

Bien qu'il n'y ait que peu de procédures à recommander, nous *recommandons* aux Administrateurs d'instituer les pratiques suivantes. Un site de Niveau 2 devrait utiliser un programme pour appliquer ces techniques. Limiter strictement les services qui tournent sur une machine. Il y en a un grand nombre préinstallés sur Windows NT. Consultez la documentation système pour leurs fonctions. Dans le doute, désactivez le service et vérifiez si tout fonctionne bien. Faites particulièrement attention aux logiciels qui incluent des services, bien que seuls des administrateurs puissent installer ces derniers. Utilisez le panneau de configuration de Services ou des outils en ligne de commande pour lister les services avant et après l'installation..

- Beaucoup de services utilisent le tout puissant compte System et peuvent ainsi compromettre la sécurité. Cependant, la plupart des services n'ont pas besoin des droits sensibles suivants, chacun d'entre eux peut complètement anéantir la sécurité d'un système :

  Sauvegarder des fichiers & des répertoires
  Restaurer des fichiers & des répertoires
  Agir en tant que partie du système d'exploitation
  Créer un objet jeton
  Déboguer des programmes
  Charger & décharger des pilotes de périphériques
  Remplacer un jeton niveau de processus
  Prendre possession des fichiers ou d'autres objets

  Servez vous de la documentation du service ou de l'éditeur pour déterminer quels droits peuvent être retirés au service. Si vous avez le moindre doute concernant le service,

[23] L'outil NETSVC du Ressource Kit de Windows NT vous permet de voir et de contrôler les services à distance, et peut être utile afin de déterminer les services qui sont actifs à travers le réseau.

lancez-le en utilisant un compte comme le “compte de service non privilégié” décrit dans les Notes qui suivent.

- Cherchez les moyens de séparer l'interaction des services les uns avec les autres. Eliminez leur interaction quand ce n'est pas une nécessité pour leur fonction. Le meilleur moyen est de lancer chaque service sous un compte unique et de s'assurer que chaque répertoire ou clé de Registre qu'ils utilisent ne sont pas accessibles aux autres.
- Sur de grands réseaux où l’administrateur ne peut pas contrôler l’installation de tous les services, utilisez un scanner de port pour vous aider à détecter les services inconnus. (Reportez vous à la section “Attaques des Services” dans *Mise en Réseau*.) Malgré tout, l’impossibilité de contrôler l’introduction des services est la racine de ce problème, et doit être la préoccupation ultime.

Examen Régulier:

Le contrôle régulier des services actifs sur chaque ordinateur sur le réseau (avec ou sans scanner de ports) est une activité de vérification importante.

Restreindre le Contrôle des Opérateurs sur les Services

Niveaux 1 & 2:

Les parties suivantes montrent à quel point les Opérateurs de Serveur peuvent aisément étendre leurs privilèges ou installer des programmes qui fonctionnent avec les pleins pouvoirs administrateurs, ce qui est contraire à la philosophie même de Windows NT :

- Le Guide *recommande* que seules les Administrateurs "Pleins Pouvoirs" installent des services en s'assurant que l' ACL de la clé de Registre suivante et son arborescence ne puissent être modifiés que par des membres des groupes Administrateurs et SYSTEM:

  ```
  HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services
  ```

  C'est une intention générale de ce Guide d'affirmer que seuls les Administrateurs " Pleins Pouvoirs " devrait être capables d'installer des applications qui fonctionnent avec des pouvoirs administratifs totaux (dans ce cas, des services).Les Opérateurs de Serveur peuvent modifier ces clefs par défaut, et c'est contraire à l'idée que les opérateurs ne puissent pas étendre leurs privilèges. Bien que les Opérateurs Serveur ont d'autres façons plus insidieuses de prendre du pouvoir[24], nous recommandons que des moyens directs comme celui ci soient retirés même au Niveau 1. Par défaut, le service de Planification qui effectue des travaux soumis via la commande AT fonctionne sous le compte SYSTEM, bien que vous puissiez le configurer autrement. (Ce service n'est pas lancé par défaut.) Un paramètre de Registre permet aux Opérateurs de Serveurs de gérer les Travaux Planifiés, ce qui leur donne la possibilité d'étendre leurs privilèges jusqu'aux Administrateurs "Pleins Pouvoirs". Dans la clé de Registre:

  ```
  HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Lsa
  ```

  La valeur nommée “SubmitControl” avec une valeur de type REG_DWORD à 1 permet cette capacité aux Opérateurs de Serveur. Si le service Planification fonctionne sous un compte dont les privilèges vont au delà de celles des Opérateurs de Serveur (en

[24] Pendant que ces Conseils essaient d'éviter que des opérateurs n'étendent leurs capacités, les Opérateurs du Serveur ont un large accès aux objets et peuvent probablement perpétrer un grand nombre de schémas de 'spoofing'. Vous devez avoir toute confiance en vos Opérateurs de serveur et être certain qu'ils n'abuserons pas de ce statut.

particulier les comptes administrateurs), nous *recommandons* que vous retiriez cette valeur. (Par défaut, elle n'est pas présente.) Voir [KBase] Q124859.

Cette contrainte signifie que seuls les Administrateurs "Pleins Pouvoirs" peuvent installer des travaux planifiés, ce qui peut être trop restrictif d'un point de vue opérationnel. *Autrement*, vous pouvez lancer le service de Planification sous un compte à qui les Opérateurs de Serveur peuvent recevoir l'accès, par exemple, un pseudo compte qui gagne ses privilèges en étant un membre des Opérateurs de Serveur. Les Opérateurs de Serveur peuvent alors être autorisés à installer des travaux planifiés.

Notes

Compte de Service non privilégié

Vous pourriez vouloir créer un “Compte de Service non privilégié”. Créez un compte local nommé, par exemple, “Service non privilégié” avec un mot de passe aléatoire de 14 caractères. Déselectionnez “L'utilisateur doit changer son mot de passe à la prochaine ouverture de session” et sélectionnez “Le mot de passe n'expire jamais.” Vous n'avez besoin de modifier aucun autre paramètre du compte. Assignez tous les Droits à ce compte à l'exception de ceux mentionnés précédemment. Configurez les services en question pour utiliser le compte non privilégié au lieu de System, ce qui leur donne nettement moins de capacités. Vous pourriez vouloir retirer d'autres Droits à ce compte, mais la liste précédente contient les plus critiques. Vous pourriez vouloir donner à ce compte des appartenances à certains groupes de tel sorte que les services qui utilisent ce compte peuvent avoir accès à certains objets, généralement l'un des compte d'Opérateurs de Windows NT ou Utilisateurs avec Pouvoirs. Remarquons cependant qu'ajouter ce compte dans certains groupes, tels que le groupe local Administrateurs, peut remettre les privilèges que vous avez retirés.

Chapitres et Sections liés:

“Attaques des Services” dans *Mise en Réseau*, pour l'importance de minimiser les services réseau.

15. Partages Réseaux

Ce guide couvre les stratégies pour le partages de répertoires et d'imprimantes. Remarquons que les utilisateurs avec pouvoirs, les Opérateurs de Serveur et les Opérateurs d'Impression peuvent créer ces partages.

Conseils

Partage de répertoires

Le partage de répertoires est le mécanisme principal pour partager des fichiers entre des ordinateurs sur un réseau Windows NT. Bien qu'il n'existe aucune procédure spécifique pour sécuriser les partages de répertoires sur le réseau, prenez en considération les indications suivantes lors de chaque nouveau partage. Remarquons que vous pouvez partager des périphériques comme les lecteur de disquette ou de CD-Roms. Ceux ci peuvent ou pas représenter un risque de sécurité excessif.

Niveaux 1 & 2:

- Réduisez au strict minimum le nombre des partages leurs ACLS . L'ACL de partage est plus forte que celle du fichier ou du répertoire car elle ne peut être modifiée par les utilisateurs du partage.
- Parce qu'un nom de partage peut être vu par des utilisateurs sans accès au partage lui même et dans certains cas à des utilisateurs non authentifiés (voir "Utilisateurs & Noms de Partages disponibles aux Utilisateurs non authentifiés" dans *Stratégies Générales*), le nom de partage ne doit pas contenir d'informations importantes, par exemple, "Contrat de fusion avec Moureaux S.A." alors qu'une fusion imminente est un secret.
- Eviter de partager le répertoire racine système (par défaut WINNT), bien que cela ne pose pas de problème de sécurité si son ACL est rigoureusement ajustée.
- Désactivez les partages administratifs si vous n'en avez pas besoin, en particulier au Niveau 2.Réferez-vous à la section "Partages Administratifs cachés" ci-dessous.
- Le répertoire NETLOGON des serveurs NT est un répertoire clé de toute politique de sécurité dans un domaine NT, ses ACL de partage ainsi que les ACL de ses sous-répertoires doivent être strictement ajustées.

Examen Régulier:

Il est particulièrement important de vérifier régulièrement l'existence des partages réseaux ainsi que leurs ACLs, étant donné que le nombre des partages ainsi que leurs ACLs tendent à augmenter avec le temps.

Accès imprimante.

Alors qu'il y' a beaucoup de raisons opérationnelles pour limiter l'utilisation des imprimantes au travers de leurs ACLs, il y a relativement peu de raisons concernant la sécurité. La sécurité physique est une préoccupation majeure pour les imprimantes parce qu'elle détermine qui peut voir ou intercepter les impressions des autres utilisateurs.

Niveau 1 & 2:

- Limitez l'accès aux imprimantes dont les documents en sortie permettraient d'augmenter les pouvoirs d'un utilisateur. Par exemple, une imprimante chargée avec des chèques blancs pré-signés ou une imprimante destinée à fournir des instructions au personnel.
- Nous *recommandons* que vous limitiez les comptes d'utilisateurs qui impriment des données sensibles avec la protection physique adéquate. Ceci aide à empêcher que ces utilisateurs évitent d'utiliser des imprimantes accessibles à tous. Alors que vous pouvez vous baser sur le respect des règles par ces utilisateurs, il est hélas facile d'envoyer un document à la mauvaise imprimante.

Remarques

Ces remarques résument quelques points essentiels concernant le contrôle d'accès à des répertoires partagés. Le partage d'imprimante réseau fonctionne de la même façon, bien que l'on se réfère de manière explicite au partage de répertoires.

Résumé des Mécanismes de Partage

- Tout ordinateur Windows NT peut présenter des partages de répertoires réseaux. Chaque nom de partage possède une ACL (qui constitue ses "permissions"). Les ACLs de partage restreignent seulement les accès distants – pas les accès à un programme sur la même machine.
- Seuls les Administrateurs, Opérateurs de Serveur et les Utilisateurs avec pouvoirs peuvent créer ou supprimer l'accès à des répertoires partagés sur le réseau, et peuvent arbitrairement modifier l' ACL des partages. Ces mêmes utilisateurs ainsi que les Opérateurs d'impression peuvent partager des imprimantes.
- Les accès distants à un fichier ou un dossier dans un partage répertoire doivent passer à la fois l'ACL du partage et l'ACL du fichier ou du dossier.
- Permettre à Tout le monde l'accès à un partage ne signifie pas nécessairement que tous les utilisateurs du réseau y auront accès, seuls ceux qui auront réussi à se loguer sur le serveur le peuvent. Malgré tout, les utilisateurs de clients autorisés peuvent voir tous les noms de partage sur une machine serveur, même ceux auxquels ils n'ont pas accès. Il y a certains cas ou les utilisateurs non authentifiés sur le serveur peuvent voir les noms de partage, bien que ne pouvant pas y accéder. Reportez vous à la section "Utilisateurs & Noms de Partage disponibles aux Utilisateurs non authentifiés" dans *Stratégies Générales*.
- Le "nom de partage," ou l'instance de partage, est celui à qui l'ACL est attachée. Si un répertoire en contient un autre et que les deux sont partagés, la seule ACL qui prime est celle que le client a référencé quand il a établi une connexion vers le partage.

Reportez-vous à la section "Comptes & Authentification Réseau" dans *Domaines & Restrictions d'Accès de Base* qui décrit comment les utilisateurs sont authentifiés pour les accès à un répertoire partagé.

Partages administratifs cachés

La clé du Registre :

```
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\
    LanManServer\Parameters
```

Peut contenir un paramètre “AutoShareServer” sur un contrôleur de domaine (“AutoShareWks” sur une Workstation). Si sa valeur est 1, le système crée automatiquement les “partages administratifs” pour ses volumes logiques, C:, D:, et ainsi de suite, qu’il nomme C$, D$… . Bien que les fenêtres d’exploration ne montrent pas ces noms aux utilisateurs, leur existence n’est pas un secret et les utilisateurs peuvent demander à s’y connecter. Sur un contrôleur de domaine, seuls les membres des groupe locaux Administrateurs, Opérateurs de Serveur, et Opérateurs de Sauvegarde (seuls Administrateurs et Opérateurs de Sauvegarde sur une Workstation) peuvent accéder à ces partages est leurs ACLs ne peuvent être changées.

Bien que les partages administratifs ne constituent pas un risque de sécurité extraordinaire même au Niveau 2, vous pouvez désactiver leur création automatique en positionnant ce paramètre à 0. Ceci peut aussi être fait au travers des Stratégies Systèmes grâce à l’option “Créer des lecteurs partagés cachés.” (Référez vous à la section Fichiers de Stratégie Système.).

Les Partages administratifs étaient faits à l’origine pour que les services systèmes puissent obtenir la place disque disponible afin d’avertir lorsqu’elle devient critique. Vous pouvez omettre la création de ces partages si vous n’avez pas besoin de ce service, cependant d’autres services peuvent en dépendre. Référez vous à la Base de Connaissance Microsoft [Q126309].

Chapitres liés:

Mise en Réseau

Fichiers de Stratégies Systèmes, création de partages réseaux cachés

Références:

[KBase] Q126309, Q158433, et Q100517.

[ConPln] Chapitre 4, *Gérer les Ressources Partagés et la Sécurité des Ressources.* Une présentation de la création et de la gestion des répertoires partagés sur le réseau.

16. Mise en Réseau

Le réseau est une part de d'environnement Windows NT et la plupart des conseils concernent sa sécurité. Ce guide offre quelques considérations générales pour l'utilisation de Windows NT dans un environnement réseau. La mise en réseau est un sujet complexe et il est difficile de donner des indications avec la même certitude que les autres parties. Nos conseils permettent aux administrateurs une considérable latitude dans cette partie, et les Notes concernent plusieurs faits notables concernant la sécurité.

Nous utilisons le terme "intranet" pour qualifier un large réseau TCP/IP. Un intranet est un assemblage de réseaux locaux TCP/IP , où chaque LAN se connecte à l'intranet au travers d'un routeur (ou une machine Windows NT jouant le rôle d'un routeur). Le travail d'un "Routeur" est d'acheminer les paquets entre l'intranet et le réseau local, ajoutant souvent certains contrôles et restrictions.

Conseils

Aucune de ces protections n'est théoriquement nécessaire sur un réseau sécurisé où aucun élément mal intentionné ne possède un accès direct, de niveau paquet au support de communication. (Voir "Ecoute sur le Réseau & Interception" dans les Notes qui suivent pour une description détaillée.) Par exemple, un petit réseau bien administré et physiquement protégé, avec seulement des ordinateurs Windows NT est raisonnablement sûre. Cependant, il est difficile de garantir que des réseaux plus vastes soient sécurisés et le restent à travers le temps. L'on devrait suivre les conseils suivant pour presque tous les réseaux d'une taille ou d'une complexité significative, en particulier si votre réseau est connecté à un réseau publique tel qu'Internet.

Niveaux 1 & 2:

- Retirez les services réseaux non nécessaires, où un "service réseaux" se réfère à un programme qui offre des services réseaux , qu'il soit ou non géré via le gestionnaire de Services. Ceci est *recommandé* pour le Niveau 1 and *prescrit* pour le Niveau 2.
- Créez et appliquer une règle spécifique pour l'utilisation des logiciels clients réseaux, par exemple, si les utilisateur doivent ou non activer Java ou ActiveX dans leurs navigateurs.
- A moins que vos systèmes Windows NT utilisent une technique particulière de cryptage comme décrit ci dessous, retirez du réseau les ordinateurs dont le système d'exploitation (voir "Ecoute sur le Réseau & Interception," ci-dessous) permet un accès direct au niveau paquet au réseau sauf si vous êtes certains que ceux ci n'utiliseront que des logiciels de confiance. Ceci est *recommandé* au Niveau 1 et *fortement recommandé* pour le Niveau 2. (C'est malheureusement plus facile à dire qu'à faire sur la majorité des réseaux. Alors que vous devrez faire des concessions, déterminez le degré de risque que représentent ces ordinateurs.)
- Empêchez Windows NT de passer des mots de passe en texte clair (texte plein, non crypté) à travers le réseau comme décrit dans la section "Mots de Passe non cryptés sur le Réseau."
- Comme décrit plus bas dans "Mots de Passe LANMAN", le format d'authentification LANMAN présente certaines faiblesses comparé au format natif de Windows NT. Si vous n'utilisez que des ordinateurs sous Windows NT alors désactivez le format LANMAN. Si vous devez utiliser des machines sous Windows 95 à travers un réseau

vulnérable, mettez la valeur de “LMCompatibilityLevel” à 1 (qui utilise le format LANMAN seulement pour les ordinateurs qui en font la requête), bien que cela induise un perte correspondante de sécurité. Au Niveau 2, nous vous *recommandons* de ne faire aucune exception : désactivez le format LANMAN.

- Isolez les services Windows NT natifs (tels que le partage de fichiers et l'administration distante) d'un intranet non sécurisé comme décrit dans “Isoler les services Windows NT natifs d'un Intranet ” dans les Notes qui suivent. Ceci est *prescrit* pour à la fois les Niveaux 1 and 2.
- Mettez un firewall entre le LAN est un intranet non sécurisé. Ceci est *recommandé* pour le Niveau 1 et *prescrit* pour le Niveau 2. La plupart des firewalls peuvent remplir les conditions de l'isolation nécessaires pour le Niveau 2. (Le critère de sélection d'un firewall va au delà du sujet de ce guide, cependant une étude complémentaire présente la Configuration de Microsoft Proxy Server.) Certains routeurs d'intranets possèdent des fonctions de sécurité et nous les avons inclus sous le terme général “firewall,” bien que la sécurité par routeur est typiquement moins puissante que celle d'un firewall.
- Beaucoup de services Windows NT et d'applications offrent des protections de cryptage contre les menaces réseaux. Utilisez pleinement ces fonctionnalités.
- Demandez la signature SMB sur tous les ordinateurs Windows NT comme décrit dans Signature SMB plus bas. Au Niveau 1, les serveurs qui doivent fournir des services aux autres ordinateurs qui ne peuvent pas faire de signature SMB peut activer mais non requérir cette signature. Sinon, la seule raison valable de ne pas utiliser de signature SMB est une dégradation des performances qui serait inacceptable pour la mission du site.
- Si votre réseau local est connecté à un intranet non sécurisé via un routeur IP (et ils les sont généralement), vous pouvez éviter que les stations locales ne communiquent avec le réseau extérieur en les configurant de telle sorte qu'elles n'utilisent que des protocoles autres que TCP/IP, comme NETBEUI. Cependant; les routeurs ou les serveurs locaux qui peuvent traduire des protocoles peuvent réduire cette protection en offrant un passage vers le réseau externe.
- Si vous utilisez un ordinateur Windows NT comme base pour un firewall vers un intranet, prenez en considération d'un paramètre de TCP/IP qui s'appelle “IP forwarding” qui transfère directement les paquets entre le réseau interne et le réseau externe. Activer l' IP forwarding réduit considérablement les contrôles de firewalls ou de routeurs imposé ailleurs.
- Finalement, et le plus important, prenez en compte les logiciels tiers qui permettent de crypter le trafic réseau (utilisateur et données systèmes) de et vers vos systèmes Windows NT. Ceci est *recommandé* pour le Niveau 2, et peut largement réduire la nécessité des autres protections dans cette liste. Voir “Appliquer le Cryptage à Tout le Trafic Réseau” dans les Notes qui suivent.

Examen Régulier:

Les menaces réseaux sont très importantes et justifient l'audit fréquent au Niveau 2.

- Mettez en place un jeu complet d'audit pour les fonctionnalités de n'importe quel firewall ou routeur avec fonctions de sécurité.
- Utilisez un scanner de port pour vérifier les services non autorisés.

Notes

Nous ne parlons pas d'attaques de Trojan ici bien qu'elles arrivent souvent à travers un réseau. Voir plutôt le chapitre *Spoofing*.

Mots de Passe non cryptés sur le Réseau

Windows NT possède la capacité de communiquer avec des systèmes non- Windows NT qui requiert l'envoi d'un mot de passe non crypté ("texte plein") à travers le réseau. Cette fonction est désactivée par défaut et doit être manuellement activée en ajoutant une chaîne nommée “EnablePlainTextPassword” avec une valeur de type REG_DWORD à 1 à la clé de Registre :

```
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\RDR
     \Parameters
```

Evitez que Windows NT n'envoie des mots de passe en clair en retirant la valeur EnablePlainTextPassword de cette clé de Registre. Cette fonction a été mise en place dans le Service Pack 3 de Windows NT 4.0 .Voir [KBase] Q166730.

Signature SMB

Windows NT supporte un mécanisme d'intégrité cryptographique appelé " Signature SMB " pour son protocole de partage natif, SMB. Windows NT utilise SMB pour accéder aux répertoires et imprimantes partagés, et un certains autres services que Windows NT fournit, comme l'administration distante. La signature SMB évite à un intrus de s'insérer dans des sessions de partages déjà établies, procédé communément appelé "hijacking de sessions". Sans signature SMB, de tels intrusions peuvent modifier et voir toutes les informations sur le serveur auquel l'utilisateur a accès. La signature SMB prévient de telles attaques. Cependant la signature SMB ne fournit aucun cryptage des données de l'utilisateur, et par conséquent tout intrus sur le réseau peut visualiser toutes le données transmises entre client et serveur.

La signature SMB fournit actuellement une protection de " 40-bit " (bien que quelques-unes de ses interactions utilisent des méthodes plus fortes). Cependant, elle utilise aussi le mot de passe de l'utilisateur comme la base de la clef de cryptage, et par conséquent la protection effective se situe entre 40-bits et l'espace du mot de passe de la clé. Pour être efficace à 40-bits, les utilisateurs doivent utiliser un plan du mot de passe qui fournit au moins un espace clé de 40 bits, ou approximativement 1012. (Voyez "Attaques par tentatives de Logon" dans le chapitre de Mots de Passe pour les calculs de l'espace du mot de passe pour les plans du mot de passe communs. Par exemple, c'est équivalent à sélectionner un mot de passe avec 7 caractères aléatoires comportant des caractères alphabétiques numériques et de casse variée.) Les versions futures de signatures SMB pourront supporter le cryptage sur 128-bit, bien que la protection effective soit encore limitée par l'espace du mot de passe.

Notez que la signature SMB permet à un intrus d'attaquer le mot de passe de l'utilisateur par force brute, bien que ce soit autant le cas pour SMB non signé. Si la signature SMB est utilisée, le mot de passe de l'utilisateur doit choisi soigneusement.

Alors qu'il s'agit d'une évolution encourageante sur la sécurité de Windows NT, il lui manque un cryptage plus performant et sa dépendance vis à vis du choix des Mots de Passe en fait une solution utile mais partielle pour la sécurité du réseau. Son effet immédiat est limiter mais en aucun cas d'éliminer les dangers d'une écoute sur le réseau.

Windows 95, les versions antérieures de Windows, et Windows NT sans cette fonctionnalités ne peuvent utiliser de signatures SMB. Si vous configurez vos serveurs pour demander la signature, ils ne pourront pas servir ces systèmes. La signature SMB augmente les temps de

réponse du réseau (bien qu'il ne réduise pas considérablement la bande passante du réseau), mais il n'y a pas d'évaluations précises publiées.

Exigez la signature SMB de l'activité d'un serveur et/ou d'un client en créant une valeur de type REG_DWORD nommée “EnableSecuritySignature” et “RequireSecuritySignature” avec un paramètre de 1 dans les clés de registre:

```
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services
   \LanManServer\Parameters

HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services
   \Rdr\Parameters
```

Cette fonctionnalité à été implémentée dans le Service Pack 3. Voir [KBase] Q161372, “How to Enable SMB Signing in Windows NT” pour les détails de sa mise en place. Si vous êtes intéressé par des aspects de ce protocole ou une discussion détaillée de ses points forts en sécurité, vous pouvez lire les articles Microsoft sur “les Protocoles d'Authentification CIFS” disponibles sur le site Web Microsoft.

Mots de passe LANMAN

Un outil qui permet de déterminer les mots de passe (L0phtcrack) a mis en évidence que le format LANMAN pour passer des informations d'authentification à travers un réseau est “considérablement” plus fragile face à un élément passif et malveillant du réseau que les techniques natives de Windows NT, bien qu'il n'y ai pas de statistiques précises sur la différence de sécurité. Globalement, ce format annule l'intérêt d'utiliser une casse de caractère différente, et limite de façon effective votre mot de passe à 7 caractères. (Les mots de passe de 14 caractères sont seulement 2 fois plus difficiles à déterminer qu'un de 7.)

Pour éviter que Windows NT n'utilise le format LANMAN, créer et positionnez la valeur de type REG_DWORD nommée “LMCompatibilityLevel” dans la clé de registre:

```
HKEY_LOCAL_MACHINE\System\CurrentControlSet\control\LSA
```

à 2, ce qui empêche Windows NT d'utiliser LANMAN. Faites cela sur tous les ordinateurs Windows NT. Remarquez qu'éliminer le format de mot de passe LANMAN signifie que certains services natifs de Windows NT (tels que les fichiers et imprimantes partagés) ne peuvent plus servir des ordinateurs sous Windows 95 où des versions antérieures. Mettre cette valeur à 1 permet de n'utiliser des formats LANMAN qu'avec des ordinateurs qui en font la demande (comme Windows 95).

Cette fonction a été implémentée dans le Service Pack 3 pour NT4. Voir [KBase] Q147706

Attaques des Services

Il y' a deux menaces réseaux majeures. La première se produit quand des utilisateurs mal intentionnés essaient d'atteindre des services auxquels ils n'ont pas normalement accès. Ces attaques de service sont contrecarrent les systèmes de sécurité en exploitant des aspects peu connus du système.

La première protection qui vient à l'esprit est d'utiliser le Panneau de configuration des Services pour retirer tous ceux qui ne sont pas nécessaires. Les sites de Niveau 2 devrait prendre le raisonnement inverse qui consiste à retirer tous les services puis à réactiver seulement ceux qui s'avèrent effectivement nécessaires. (Voir *Services Systèmes*.)

Même après une installation initiale de Windows NT qui réduit les services, les applications ajoutés au système peuvent mettre en place leurs propres services réseaux, ceux ci offrent bien souvent des sécurités modestes. Vous pouvez utiliser un “scanner de port” pour trouver

de tels services.[25] Les scanners de ports sont des logiciels qui tentent de se connecter à des ports TCP ou d'autres protocoles que les services emploient pour remplir les fonctions fournies aux clients. Alors que le scanner ne peut généralement pas identifier le service, il peut au moins reporter qu'un certain service remplissait une requête sur un certain port, ce qui aide à trouver des services non autorisés sur le réseau. En outre, un grand nombre de services utilisent des ports universellement connus, ce qui peut aider à identifier le service en question.

La meilleure protection pour un réseau connecté à un intranet non sécurisé est d'interposer un firewall entre le LAN et l'intranet. Une autre étude pour ce projet offre des Conseils pour la configuration sécurisée de Microsoft Proxy Server qui est considéré comme un firewall.

Ecoute sur le Réseau & Interception

La seconde menace réseau se produit lorsque des éléments malveillant sur un réseau qui peuvent « écouter » ou intercepter des données entre deux communicants légitimes. La plupart des media de communication réseau sont prédisposés à l'écoute et à l'interception. Des ordinateurs sur le réseau sont capables de lire ou même intercepter des paquets, les changer, et rerouter les faux paquets au récepteur prévu.

Une Usurpation de Session (“Session hijacking”) est un type particulier d'attaque qu'il est possible d'entreprendre sur Windows NT. Quand un client Windows NT se connecte à un partage réseau du serveur, le serveur authentifie l'utilisateur sans faire passer aucun Mots de passe à travers le réseau. (Le client et le serveur utilisent une technique “challenge/response” classique.[26]) Une fois que le serveur authentifie l'utilisateur client, le serveur fait passer un identifiant de session non protégé au client. Le client présente par la suite cet identifiant pour toutes les demandes ultérieures de connexion à un répertoire partage sur le même serveur sans autre authentification.

Une Usurpation de Session se produit quand un agresseur actif lit l'identifiant et par la suite présente les demandes au serveur. Le serveur les considérera comme des demandes légitimes et les traitera. Cette attaque réussit non parce que Windows NT a des défauts de sécurité, mais seulement parce que le trafic réseau n'est pas protégé par des techniques de cryptographie. On peut trouver différentes variantes de cette attaque sur la plupart des systèmes d'exploitation réseau qui n'utilisent pas de telles techniques. Nous précisons que cette attaque souligne seulement la vulnérabilité d'un réseau non protégé par la cryptographie.

Pour effectuer de telles attaques, un programme malintentionné a besoin d'un accès direct au matériel réseau de l'ordinateur. Windows NT et des systèmes tels qu'UNIX (toutes les versions majeures), VMS de Digital, et AS/400 sont conçus pour interdire à des programmes non privilégiés un tel accès. Lorsqu'ils sont convenablement administrés (et au delà de toute défaillance de sécurité) ces systèmes ne posent pas de tels risques sur le réseau. Cependant, tous les programmes sur des systèmes tels que DOS, Windows (versions autres que Windows NT), et Macintosh possèdent de tels accès.

Les techniques de cryptographie fournissent la seule protection efficace contre ces attaques par le réseau. De telles techniques peuvent assurer que les paquets « écoutés » ne peuvent être décodés et que les paquets modifiés de façon malintentionnée peuvent être efficacement et

---

[25] Les scanners de port fonctionnent typiquement sur le protocole IP. L'outil NETSVC du ressource kit Windows NT Server vous permet d'interroger et de contrôler les services à distance, et peuvent aussi être utiles pour déterminer quels services sont actifs à travers le réseau.

[26] Remarquons cependant qu'un élément réseau malveillant peut observer la paire challenge/réponse pour monter une attaque en force brute sur le mot de passe.

immédiatement détectés. Windows NT ne fournit pas de telles protections. Toutefois, vous pourrez acquérir les produits de sociétés tierces qui le font pour toutes les communications NT-à-NT, ou pour des applications spécifiques comme le trafic entre les explorateurs et les serveurs Web.

Appliquer le Cryptage à tout le Trafic Réseau

Les techniques de cryptage fournissent la seule protection efficace contre les attaques actives ou passives sur le réseau (écoute et interception). Certains services et applications réseau Windows NT fournisse une telle protection, mais pas tous. Notre Guide recommande à tous les systèmes Windows NT de niveau 2 d'appliquer une protection[27] réseau cryptographique à l'aide d'outils tiers pour tous le trafic (c'est à dire, le trafic données de l'utilisateur aussi bien que le trafic système de Windows NT) dans les situations suivantes:

- Des réseaux WAN Windows NT qui utilisent des intranets peu sûrs pour leurs communications entre les différentes enclaves Windows NT. Notez que les firewalls qui ne cryptent pas ne se protègent pas eux mêmes contre ces menaces d'écoute.
- Quand le réseau Windows NT contient des ordinateurs dont les systèmes d'exploitation ne peuvent empêcher les programmes d'accéder directement, au niveau des paquets, au réseau. Ceux ci comprennent DOS, Windows (toutes les versions excepté Windows NT), et Macintosh. Quand il est correctement configuré et administré, UNIX (toutes les variétés principales), Digital VMS, AS/400, et la plupart des systèmes d exploitation “basé-kernel ” prétendent empêcher un tel accès direct. (Toutefois, les systèmes d' exploitation “free” comme Linux et FreeBSD seront peut-être plus facile à exploiter du au fait de la disponibilité des codes sources du kernel.)
- Quand n importe quel élément du mécanisme de transport de communications est enclins à l'écoute ou l'interception, comme lors de l'utilisation d'un média publique.

La protection cryptographique devrait contenir un cryptage (qui assure que les intrus ne peuvent voir les informations) et un contrôle d'intégrité (qui permet la détection des données modifiées).

Isoler le Service Natif Windows NT de l'Intranet

Il y a de nombreux dangers lorsque votre LAN Windows NT fait partie d'un intranet, et les attaques sur les services natifs de partage de Windows NT sont l'un de ces risques. Les services natifs de partage de Windows NT comprennent le partage d'impression et des fichiers, et un mécanisme appelé “named pipes”(canaux nommés) qui sert de base pour de nombreux services client-serveur, par exemple la majorité de l administration distante de Windows NT. Il y a deux techniques pour être sûre que les sources sur l’intranet ne puissent interférer ou écouter ces services natifs.

La première technique est d'utiliser uniquement le protocole NETBEUI pour ces services natifs. Les paquets du protocole NETBEUI ne peuvent être routés sur ou reçus de l'intranet par la plupart des routeurs. En supposant que vous ayez déjà installé le protocole NETBEUI, utilisez le panneau de configuration Réseau pour vous assurez que les services suivants sont affectés au protocole NETBEUI: Interface NetBIOS, Serveur, et Station de Travail. Faites ceci sur tous les ordinateurs Windows NT présents sur votre LAN. (Voir « Isoler les Services NT d'un Intranet” dans le Chapitre *L’Internet et Intranets* dans [Sutt96], pp. 255-257.)

---

[27] Voir, par exemple, le produit “SnareNet” de Snare Networks Corp. (http://www.snare.com).

Une deuxième technique répandue bloque ces services au niveau du routeur. Ces services natifs peuvent aussi utiliser le protocole TCP/IP qui est routable à partir de l'intranet. Toutefois, ils utilisent uniquement les ports UDP et TCP de 137 a 139, et par convention, les communicants sur les réseaux TCP/IP ne se servent de ces ports pour aucun autre rôle. De nombreux routeurs peuvent identifier et bloquer les numéros de ports TCP et UDP désignés, et ils peuvent donc assurer que les éléments sur l'intranet ne peuvent interagir avec les services natifs Windows NT sur le LAN. Bloquez simplement à la fois les ports UDP et TCP numérotés 137-139. Les détails dépendent évidemment de chaque routeur. L'avantage de cette seconde technique est que vous administrez seulement le routeur au lieu de tous les ordinateurs sur le LAN. Il vous laisse aussi utiliser TCP/IP sur le LAN pour ces services.

Evidemment, cela signifie que les ordinateurs sur le LAN ne peuvent plus demander ou offrir ces services natifs Windows NT à des ordinateurs sur l'intranet. Si vous avez besoin de cette capacité, vous devriez vous procurez les packs cryptographiques tiers qui le permettent.

Spoofing IP

De nombreux packs de sécurité Windows NT peuvent filtrer les paquets à destination ou venant d'un intranet en se basant sur l'adresse IP source/destination. Toutefois, des éléments sur un réseau incertain peuvent souvent insérer n'importe quelle adresse IP dans les paquets qu'ils envoient, et interceptent les paquets quel que soit l'adresse IP d'envoi ou de réception. Ceci est appelé l' "IP spoofing" et cela réduit les effets du filtrage IP en tant que protection efficace. Il y' a des efforts de standardisation sous-jacents pour contrer cette menace en utilisant des techniques cryptographiques. Aussi, les packs de cryptage réseau tiers contrent efficacement le spoofing IP. Les sites Windows NT de niveau 2 ne devraient pas se contenter d'un simple filtrage IP pour la sécurité dans des environnements intranets hostiles.

Limitation des Ports TCP/IP

Les options de sécurité avancées dans la configuration du protocole TCP/IP (accessible à travers le panneau Réseau) peuvent restreindre le trafic TCP et UDP à une liste spécifique de ports. Cependant, alors que les services utilisent fréquemment des numéros de ports fixes, les clients peuvent utiliser une grande variété de ports. Nous vous recommandons d'explorer cette fonction afin d'ajuster les ports disponibles aux programmes. Ceci est une fonction avancée et opérationnelle de TCP/IP qui va au delà de notre sujet actuel, et ces conseils n'offrent par de directions spécifiques.

La Sécurité des Protocoles de Windows NT

Il n'y a pas de sécurité inhérente et significative dans les protocoles natifs de Windows NT : NETBEUI, TCP/IP, et IPX/SPX, et il n'y a pas d'avantage significatif à utiliser l'un plutôt que l'autre, à part comme indiqué ci-dessus.

Chapitres et Sections liés:

Conseils pour Sécuriser Microsoft Proxy Server, un document accompagnant ce Guide.

Services Systèmes, pour réduire les services réseaux systèmes.

Service d'Accès Distant (RAS)

Références:

[Kauf95] Une excellente présentation des problèmes de sécurité sur un réseau.

[Shel97] Chapitre 15, *Sécurisations des WANs privés et des WANs Virtuels.*

[Shel97] Chapitre 18, *Firewalls et Serveurs Proxy*.

[Sutt96] Sujet Intranets dans le Chapitre 3, *Votre Environnement de Travail*, p. 53-55.

[Sutt96] Chapitre 9, *Internet et Intranets*, p. 225, excepté le sujet “Internet Information Server.”

17. Service d'accès distant (RAS)

Les lecteurs nouveaux aux principes du Service d'Accès Distant devraient d'abord lire les références mentionnées à la fin du guide.

Le service d'accès distant de Windows NT (RAS) permet à des ordinateurs distants de se connecter au serveur d'accès distant à travers une ligne téléphonique ou, en utilisant le protocole PPTP, à travers un intranet. Une fois connecté, l'ordinateur client fonctionne comme s'il était directement attaché au LAN sur serveur RAS. Par exemple, le client peut se connecter à un répertoire partagé et utiliser l'imprimante sur le réseau, étant soumis aux règles normales de contrôle de sécurité sous Windows NT. RAS peut être limité à un certain nombre d'utilisateurs, et possède une fonction de rappel ("call-back") ou le serveur rappelle un numéro de téléphone prédéterminé ou celui d'un utilisateur spécifié pour achever le scénario de connexion. La sécurité du Service d'accès distant est étroitement intégrée à l'architecture de sécurité de domaine Windows NT. Le client RAS est disponible pour d'autres systèmes d'exploitation, comme Windows 95.

Remarque: L'accès distant à votre réseau via une connexion ou au travers un intranet ouvre beaucoup de portes à des attaques, dues en partie au manque de protection physique de l'ordinateur distant. (Référez-vous aux Remarques ci-dessous.) Bien que les indications suivantes dénombrent beaucoup de ces attaques, vous devriez peser avec attention les avantages et les risques d'un accès distant. Beaucoup de sites, en particulier ceux qui sont conformes aux spécifications du Niveau 2, n'utilisent pas l'accès distant.

Conseils

Niveau 1:

- Nécessite l'activation de "L'authentification cryptée Microsoft " sur le serveur RAS et sur tous les clients. Ceci assure que des mots de passe non crypté ne transiterons jamais sur le système de communication.
- Si vous utilisez RAS au travers de lignes téléphoniques qui puissent être susceptibles d'être écoutées, ou si vous avec PPTP à travers un intranet peu sécurisé, demandez le cryptage des données à la fois sur le serveur et le client. Si votre version de Windows NT le permet, choisissez le cryptage 128-bits plutôt que le défaut de 40-bits. (Voir les notes qui suivent)
- Donnez les droits d'accès distant à seulement ceux qui en ont le besoin. (Utilisez le panneau "Numérotation" à partir du gestionnaire des utilisateurs, ou la fenêtre d'administration du Service d'accès Distant. Ils sont équivalents.)
- Quand cela est possible, utilisez le rappel vers un numéro prédéfini (donc un numéro qui ne peut pas être spécifié par l'utilisateur).
- Assurez-vous que les mots de passe des utilisateurs sont d'une complexité suffisante. Référez-vous à la section "Mots de passe utilisateurs Solides" dans les remarques qui suivent.
- N'utilisez pas de clients RAS sur des systèmes d'exploitation autres que Windows NT, sauf si vous savez que ce système d'exploitation est assez sécurisé pour se connecter directement sur votre réseau. Cependant, il n'y a aucune façon pour le serveur RAS

d'imposer que les clients soient sous Windows NT. Dans tous les cas, nous vous recommandons de n'utiliser que des clients Windows NT clients.

- Prenez en considération la configuration de la "Sentinelle RAS" décrites dans les Notes.
- Nous vous *recommandons* d'examiner l'ajout d'un second système d'authentification pour protéger les accès distants. (Voir la page 373 dans [Shel97] pour une liste de tels systèmes.)

Niveau 2:

Les mêmes indications qu'au Niveau 1 avec les améliorations suivantes:

- Assurez-vous que l'ordinateur distant est physiquement protégé. (Référez-vous aux remarques ci-dessous)
- N'utilisez pas de clients RAS autres que Windows NT.
- Ne comptez pas sur le cryptage de données 40-bits.
- Utilisez le rappel vers un numéro prédéfini sauf si les risques d'attaque sont manifestement très faibles.

Examen Régulier:

Parce que les menaces externes sont particulièrement dangereuses, nous vous conseillons de pratiquer des revues régulières.

- Vérifiez les utilisateurs qui ont un accès distant et qui ne l'utilisent pas activement.
- Assurez-vous que le rappel est utilisé à chaque fois que cela est possible.
- Vérifiez la sécurité physique des ordinateurs distants.

Remarques

Considérations Générales

L'accès distant est souvent sur les sites le système le moins protégé en comparaison de l'accès direct au réseau local, et ceci présente un risque significatif que vous devez prendre en considération. Beaucoup de manières existent pour compromettre la sécurité d'un système en ayant physiquement accès à un ordinateur distant. Alors qu'il n'y a pas de guide absolu à ce niveau, vous devez attacher une grande importance à la sécurité des machines distantes, et ce plus particulièrement au Niveau 2. (Vous pouvez, par exemple, booter à partir d'un disque amovible qui peut être disposé ailleurs lorsqu'il n'est pas utilisé.)

Les restrictions des exportations aux Etats-Unis imposent une limite de cryptage de 40 bits sous Windows NT. Cependant, les utilisateurs Américains peuvent obtenir un cryptage 128-bits directement de Microsoft ou d'un fournisseur tiers. Le cryptage 40-bits permet une protection relativement modeste contre les attaques. Le cryptage 128-bits est impossible à casser en utilisant des techniques de 'force brute'—à l'exception de faiblesses éventuelles dans son algorithme. Les versions actuelles du Service d'accès distant Microsoft utilisent l'algorithme RC4 de RSA, Inc., qui n'a pas de faiblesses connues.

Vous pouvez limiter l'accès distant au seul serveur RAS, en opposition au réseau auquel le serveur est rattaché. (Par exemple, avec cette limitation, un utilisateur distant peut accéder à des fichiers sur le serveur RAS mais pas à des répertoires partagés sur le réseau.) Il s'agit d'une restriction sensible pour les utilisateurs qui n'ont pas besoin d'un accès au réseau. C'est aussi une couche de protection effective pour le réseau. Soulignons que des comptes

individuels peuvent être restreints au seul serveur RAS en les déclarant comme comptes locaux. Sur un réseau Windows NT, les comptes locaux peuvent seulement accéder à l'ordinateur qui contient le compte, le serveur RAS dans le cas présent.

Le paramètre NetbiosGatewayEnabled du Registre dans la clé:

```
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services
      \RemoteAccess\Parameters\NetbiosGateway
```

contrôle cet accès au réseau en général. Cependant, ne positionnez ce paramètre qu'au travers du programme de configuration du Service d'Accès Distant. Ces idées sont la base de la 'Sentinelle RAS' décrites plus bas.

Il existe un certain nombre de paramètres du Service d'accès distant qui peuvent êtres activés par l'utilisateur client, par exemple demander une communication cryptée. Les serveurs RAS imposent généralement les paramètres importants de sécurité et ne dépendent pas du paramétrage des clients. Cependant, c'est une bonne habitude que de configurer les clients pour "Accepter seulement les authentifications cryptées Microsoft" ainsi que le même niveau de cryptage des données sur l'hôte.

L'utilisateur client a le choix de laisser le système "sauvegarder" son mot de passe qui sera fournit automatiquement lors de connexions ultérieures. Ce Guide prend pour position qu'il n'y a pas d'avantages de sécurité particuliers à sauvegarder ou non. Bien que le fait de sauvegarder les Mots de passe ajoute une charge à Windows NT, qui est de protéger le mot de passe, le fait de saisir le mot de passe pendant une connexion (requis quand ils ne sont pas sauvegardés) ne se fait pas toujours selon un "Trusted Path". La pratique client la plus sûre est d'utiliser l'option "connexion en utilisant l'accès réseau à distance" dans la fenêtre de connexion et alors de ne jamais sauvegarde le mot de passe lorsque l'on vous le propose. Dans ce scénario, vous entrez votre mot de passe via un "Trusted Path" – la fenêtre normal de connexion. Toutefois, un administrateur n'a pas de moyen particulier de forcer les utilisateurs à procéder de cette manière.

Il y' a un certain nombre de paramètre de contrôle pour le Service d'accès distant dans la clé de registre :

```
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services
      \RemoteAccess\Parameters
```

dont les valeurs par défaut conviennent pour des sites de Niveaux 1 et 2. Ceux-ci incluent le paramètre qui informe le Service d'accès distant d'auditer ses transactions dans le journal sécurité, ce qui est activé par défaut.

Mots de passe Utilisateurs Solides

Microsoft ne publie pas habituellement les détails de leurs protocoles de cryptographie et nous n'avons pas réussi à trouver une documentation officielle pour cette étude. Cependant, il semble évident que le mot de passe de l'utilisateur est la base du cryptage RAS et il y a ainsi des preuves anecdotiques qui appuient cette hypothèse. Si cela est vrai, cela n'expose pas seulement le mot de passe utilisateur aux attaques par force brute sur le canal de communication mais limite effectivement la force de ce cryptage RAS à la longueur du mot de passe de l'utilisateur. Il est donc important de se servir de mots de passe aléatoires dont la taille est au moins aussi longue que la longueur de la clé cryptographique désirée. Voir "Signature SMB" dans *Mise en réseau* pour une discussion sur la complexité du mot de passe utilisateur quand il sert de base aux clés cryptographiques.

Par ailleurs, un intrus qui cherche à déterminer la clé de cryptage d'une connexion RAS par force brute voudrait simplement utiliser une technique classique d'attaque de mots de passe

en générant chaque clé d'essai à partir d'un mot de passe de test. (La clé RAS est une sorte de "hash" du mot de passe actuel de l'utilisateur, mais nous présumons que l'intrus sait générer une clé de test à partir d'un mot de passe donné.) Et dès lors que la clé de cryptage est découverte, alors il en est de même pour le mot de passe de l'utilisateur!

Sentinelle RAS

Une Sentinelle RAS est un nom que nous donnons à un serveur RAS conçu pour maximiser l'isolation vers le réseau principal. Pour mettre en place une Sentinelle RAS:

- Installez un serveur RAS sur un contrôleur de domaine Windows NT dédié en accord avec les Conseils plus haut. Restreignez l'accès à distance au serveur RAS lui même – ne permettez pas l'accès à distance sur le réseau du serveur.
- Créez un compte de domaine sur la sentinelle RAS pour chaque utilisateur qui a besoin de l'accès à distance. (Ceci en plus de leur compte quotidien dont ils se servent pour leur ordinateur sur site, mais il pourrait utiliser le même nom de compte.) Créez des Mots de passe puissants basés sur “Attaques par Mots de Passe capturés” dans *Mots de passe*. Nous recommandons que vous attribuiez de tels Mots de passe aux utilisateurs et que vous ne les laissiez pas modifier ces Mots de passe. Assignez des capacités RAS au compte.
- Mettez en place un répertoire personnel sur le serveur RAS pour chacun de ces utilisateurs et partagez-le sur le réseau de telle sorte que les utilisateurs puissent accéder à leur répertoire à partir de leurs stations habituelles sur le site.
- Configurez le contrôleur de domaine RAS pour autoriser les autres domaines dont les utilisateurs ont besoin pour transférer des données à partir ou vers la sentinelle RAS. En général ce sont des domaines qui contiennent les comptes sur sites pour les utilisateurs pour qui vous avez configuré les comptes sur la sentinelle RAS. Notez que les comptes à distance RAS ne sont pas reconnus sur les ordinateurs autres que la sentinelle RAS, ce qui minimise les dommages potentiels qu'ils peuvent faire sur le réseau.
- Minimisez les services et les applications qui sont exécutées sur la sentinelle RAS. Il est aussi mieux de simplifier la sentinelle RAS en général. Par exemple, ne vous en servez pas pour fournir des données générales ou des services d'impression pour les ordinateurs sur le réseau.
- Activez le plus d'audit que vous pouvez traiter et surveiller.

Les utilisateurs n'ont pas d'accès direct du site distant vers n'importe quel ordinateur sur le réseau. Généralement, ils utilisent la sentinelle RAS en transférant des données de et vers des stations sur le site, puis en travaillant sur ces fichiers à distance.

Références:

[Sutt96] *Utiliser le Service d'Accès Distant*, p. 118, et *RAS et PPTP*, p. 252.

[NetSp] Chapitre 5-7 sur Remote Access Service (RAS). Présentation et procédures générales pour administrer RAS.

[TchNet] Article intitulé “MS Windows NT Server 3.5 Remote Access Service.” Une introduction aux capacités et à la technologie de RAS.

18. Spoofing

Chacun des programmes sous Windows NT permet à l'utilisateur d'obtenir un maximum de droits. Si un utilisateur n'ayant pas certains droits peut créer des programmes malveillants lui permettant d'avoir un second utilisateur qui aurait plus de droit, le premier utilisateur peut ainsi étendre ses propres droits par le deuxième utilisateur. Cela est appelé communément le « spoofing » est c'est particulièrement dangereux quand le second utilisateur est un administrateur. De tels programmes malveillants sont introduits dans le système en tant que programmes bénins. C'est le « Cheval de Troyes ». Ces programmes sont aussi appelés « virus », ce terme est devenu commun.

Les utilisateurs avec des droits de sécurité spéciaux (que l'on appelle normalement « administrateur ») doivent être particulièrement vigilants et n'utiliser que des programmes dont le ACL les protège contre le remplacement total ou partiel par des utilisateurs ayant de moindres droits. Malheureusement, cela peut être difficile à vérifier. Beaucoup de caractéristiques d'un système d'exploitation tel que Windows NT sont spécialement conçues pour permettre l'exécution facile, transparente et flexible des programmes, chacun d'entre eux pouvant être un programme de spoofing potentiel.

Le spoofing est peut-être le plus gros risque de sécurité que vos allez rencontrer. Le confiner requiert une collection de tâches difficiles, diverses et non-spécifiques. Nous présentons dans cette section plusieurs d'entre elles, mais il y en a d'autres, sans aucun doute.

Un des meilleurs moyens de minimiser les risques de spoofing et de minimiser la quantité de travail faisable par les utilisateurs, et particulièrement les administrateurs « pleins pouvoirs ». C'est un des buts principaux de la section concernant les « Administrateurs de Domaine & Utilisateurs avec Pouvoirs » dans *Structure Administrative*. Un autre bon moyen est d'effectuer l'administration du système à distance, à partir d'une station de travail limitée, protégée, configurée au minimum et dédiée à l'administration (voir « Le compte Administrateur » dans *Structure Administrative*).

Le fait de spoofer un utilisateur normal peut résulter en l'exposition ou la modification non-détectée de leurs propres fichiers ou de ceux dépendant de leur groupe de contrôle. Alors que cela n'est pas aussi dangereux que pour les administrateurs, cela pose un cas délicat pour les utilisateurs qui possèdent des informations sensibles et que la même protection est appliquée.

Notez bien que les conseils contenus dans ce chapitre sont liées avec ceux dans Conseils & Notes. Les conseils listés correspondent aux notes du paragraphe précédent.

Conseils & Notes

Séparation de Sessions

Le moyen le plus sûr d'éviter qu'un utilisateur ne puisse en spoofer un autre et de s'assurer que chacun d'eux ne peut pas s'identifier sur la même machine que l'autre (au travers du premier ou second identificateur), ou que le premier n'ait que le droit de Lire dans le Registre et le système de fichiers dans l'espace de travail dans lequel le deuxième travaille. Nous ne pouvons pas donner de conseils spécifiques autres que le fait de considérer la confiance que vous accordez aux utilisateurs qui accèdent aux ordinateurs.

Trusted Path (“Fenêtre Sécurité,” “Secure Attention Sequence”)

Quand vous utilisez la combinaison de touches CTRL+ALT+DEL pour appeler la fenêtre de Sécurité de Windows NT , vous utilisez ce que l’on appelle généralement « Trusted Path » (Chemin de Confiance), « Secure Attention Sequence », ou « Security Window ». Le «Trusted Path» est une action physique que chaque utilisateur peut faire pour être certain que toute interaction avec l’ordinateur (une fenêtre dans ce cas) est garantie d’être légitime, et que cette fenêtre correspond bien à une vraie fenêtre et non pas à une application sous le contrôle d’un programme malveillant. Les interactions sensibles, comme entrer un mot de passe, sont traditionnellement dans un «Trusted Path » et Windows NT continue cette tradition. L’utilisateur doit consciencieusement utiliser le «Trusted Path» pour se connecter, se déconnecter, modifier son mot de passe, et bloquer sa station de travail. Le Menu Démarrer n’en est pas un. Cependant, de par le fait que le bureau dans Windows NT est de manière inhérente mono-utilisateur, un utilisateur a donc peu de chance de présenter un faux Menu Démarrer à un autre, ou même modifier le Menu Démarrer d’un utilisateur. Un programme malveillant doit tourner sous la session de l’utilisateur actuel afin de présenter un faux Menu Démarrer. De tels programmes ont déjà un accès total aux données de l’utilisateur et à son environnement, et spoofer son Menu Démarrer donnerait au programme le peu qui lui manquerait. Un programme malveillant, dans cette situation, peut mettre en place des éléments dangereux de façon permanente dans l'environnement de l'utilisateur, mais il y a beaucoup d’autres moyens de faire cela sans altérer le Menu Démarrer.

La pratique de lutte contre le spoofing doit toujours chercher à préserver l'utilisateur de certains programmes qui pourraient présenter un faux menu Démarrer ou tout autre élément du bureau en premier. Une fois qu'un tel programme est lancé, la bataille est en général déjà perdue.

Variable “PATH” et autres variables d'environnement

La variable d'environnement "PATH" définit une liste de répertoires où la fenêtre DOS et les autres éléments du système recherchent des commandes tapées par l'utilisateur. Le PATH doit non seulement contenir les répertoires dont l'ACL empêche les utilisateurs douteux d'ajouter ou de modifier des fichiers, principalement les exécutables et les bibliothèques dynamiques (DLL), mais aussi n'importe quel fichier dont un programme légitime puisse avoir besoin. Les utilisateurs peuvent modifier leur variable "PATH" personnelle mais devraient être avertis afin de suivre ce conseil.

Si l'option est activée dans le Registre, le système parcours l'AUTOEXEC.BAT, cherchant et ajoutant les chemins qui s'y trouvent dans une variable PATH de l'utilisateur qui s'est loggué. La valeur nommée " ParseAutoexec " avec une valeur de type REG_DWORD à 1 dans la clé:

```
HKEY_CURRENT_USER\ Software\Microsoft\Windows NT\
     CurrentVersion\Winlogon
```

active ceci (activée par défaut). Bien que n'importe quel utilisateur soit autorisé à activer cette clé dans son propre environnement, la clé n'est accessible que par cet utilisateur et est à l'abri d'une attaque. Cependant, l'AUTOEXEC.BAT doit être protégé si un utilisateur active cette clé. Notez que l'Editeur de stratégie système peut modifier la valeur de celle-ci lors de l'ouverture de session de l'utilisateur, bien qu'il n'empêche pas les utilisateurs de changer sa valeur durant leur session.

Les autres variables d'environnement peuvent fournir des occasions de spoofing, mais les utilisateurs généraux ne peuvent pas modifier les variables d'autres utilisateurs parce qu'elles sont stockées dans le profil de celui-ci. Cependant, les administrateurs devraient faire attention lorsqu'ils définissent des variables d'environnement système globales. (Utilisez

l'onglet "Environnement" dans l'icône Système du panneau de configuration pour visualiser et définir les variables d'environnement système ainsi que celles de l'utilisateur).

Conseils:

Niveaux 1 & 2:

- Assurez-vous que la variable d'environnement globale PATH contienne uniquement des répertoires d'applications en accord avec les conseils de "Répertoires d'Application" dans *Applications & Répertoires Utilisateurs*.
- Positionnez l'ACL sur l'AUTOEXEC.BAT comme décrit dans la partie *Système de Fichier & ACL du Registre*.
- N'ajoutez ou ne modifiez pas de variables d'environnement système sans avoir la certitude que leur valeur n'entraîne pas de risque de spoofing.
- Réduisez au strict minimum le chemin de recherche des administrateurs et opérateurs, confinez les à des répertoires protégés qui contiennent seulement des programmes dignes de confiance.

Le Problème du "."

La fenêtre DOS effectue une recherche implicite de la commande entrée dans le répertoire courant (c'est à dire ".") avant de la rechercher dans le PATH, ce qui expose à une grande menace de spoofing qu'il est difficile de maîtriser. Les API de Windows NT qui autorisent une application à en exécuter une autre (comme CreateProcess) recherchent l'application à exécuter d'abord dans le répertoire courant puis dans le PATH. (Dans les deux cas, le système peut exécuter des programmes dont l'extension est autre que .EXE, mais seulement lorsque leur nom complet est spécifié). Ces mêmes remarques pour les fichiers .EXE s'appliquent aux fichiers batch d' extension.BAT et à ceux d'extension .COM. Il y a beaucoup d'endroits dans Windows NT ainsi que ses applications qui autorisent les utilisateurs à exécuter d'autres programmes, et il est très difficile de dire où ils recherchent ces programmes. Il est très difficile de se protéger contre cette méthode de spoofing. Quelques suggestions:

1. Considérez l'emploi d'outils tiers pour la ligne de commande qui permettent d'éviter de chercher le répertoire courant (“.”). (Parce qu'UNIX a traditionnellement cette capacité, les suites de commandes “shell” UNIX peuvent être intéressantes.) Celles-ci sont particulièrement importantes pour les administrateurs utilisant les fenêtres de commandes.
2. Surveillez la présence d'exécutables dont l'ACL indique qu'ils ont été créés par d'autres utilisateurs que ceux autorisés. Les fichiers dont les noms sont les mêmes que la plupart des commandes système nécessitent une attention toute particulière.
3. Evitez de travailler dans des répertoires où les utilisateurs de capacités plus réduites peuvent créer de nouveaux fichiers, en modifier ou changer l'ACL de fichiers existants.
4. Dans la mesure du possible, utilisez la commande Exécuter du menu Démarrer, ou le Gestionnaire de tâches obtenu au travers de la fenêtre Sécurité (Trusted Path). Celles-ci effectuent une recherche dans le PATH mais pas dans le répertoire de travail courant. Malheureusement, elles ne se révèlent pas souvent très pratiques lorsque vous travaillez dans une fenêtre de commande.
5. Surveillez la présence de fichiers dont l'extension est .EXE, .BAT, ou .COM dont les propriétaires sont d'autres utilisateurs que ceux autorisés à installer des applications (Voir "Répertoires d'Applications" dans Applications & Répertoires Utilisateurs).

Cependant, notez que cette menace est à peu près équivalente à un intrus qui placerait simplement un fichier dans un répertoire que les utilisateurs pourraient "ouvrir" aisément, souvent par un double-clique.

Conseils:

Niveaux 1 & 2:

Les pratiques précédentes sont *recommandés*.

Fichiers de données contenant des programmes cachés

Beaucoup d'applications permettent à leurs documents de contenir des données qui peuvent s'exécuter comme un programme dans certains cas. Un utilisateur naïf qui "ouvrirait" simplement un tel document pourrait déclencher ces programmes qui souvent sont exécutés et demeurent inaperçus. C'est une occasion de spoofing virulent.

L'exemple le plus connu est celui des "macro" virus dans les applications telles que Word de Microsoft. Un utilisateur peut attacher des programmes écrits dans un langage de programmation souple à des documents et que l'utilisateur active via certaines combinaisons de touches ou simplement en ouvrant ou en sauvegardant le document. Comme toujours, de tels macros s'exécutent avec les pleines capacités de l'utilisateur trompé.

Examinez soigneusement la documentation d'une nouvelle application afin de déterminer des problèmes potentiels avant que vous ne l'installiez. Quelquefois vous pourrez désactiver certaines fonctionnalités qui pourraient s'avérer dangereuses. Sinon, informez vos utilisateurs sur les dangers et précautions à prendre lorsqu'ils utilisent ces programmes. Sauf en cas d'absolue nécessité, retirez le droit d'accès à ces programmes " X " aux administrateurs afin qu'ils ne puissent pas les lancer accidentellement.

Conseils:

Niveaux 1 & 2:

- N'installez pas d'applications sur le système jusqu'à ce que vous ayez déterminé si elles présentent ou non cette menace.

Les programmes d'exécution automatique sur CD-ROM

Les CD-Roms peuvent contenir un programme d'exécution automatique qui est lancés lors de l'insertion du CD-ROM dans le lecteur ou lorsque l'on double clique (pour l'ouvrir) sur l'icône du CD-ROM dans le bureau. Heureusement, cela ne se produit pas lorsque vous vous loguez sur un ordinateur et qu'un CD est présent dans le lecteur, ce qui serait une occasion de spoofing (trop) facile et efficace. Comme pour les autres risques de spoofing, les programmes d'execution automatique mal-intentionnés peuvent être invisibles ou paraître bénins. La clé du Registre:

```
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Sevices\Cdrom
```

peut contenir une valeur de type REG_DWORD nommée " Autorun " qui contrôle cette fonctionnalité. Mettez sa valeur à 0 pour désactiver l'exécution automatique. En outre, un utilisateur peut se servir de la touche “SHIFT” pour éviter le lancement automatique au moment où il devrait être activé. (Voir [KBase] Q155217 et Q126309.)

Conseils:

Niveaux 1 & 2:

- Désactivez le lancement automatique sur tous les systèmes au Niveau 2, et sur les Contrôleurs de Domaine et les serveurs principaux au Niveau 1. Bien que nous *recommandons* que vous le désactiviez même au Niveau 1, vous pouvez le laisser activé si cela fournit une fonctionnalité utile sur le site, et si vous apprenez aux utilisateurs les dangers d'un CD-Rom peu sûr et comment déjouer le lancement automatique en utilisant la touche SHIFT.

Spoofing de Raccourcis

Si un utilisateur peut redéfinir les propriétés du raccourci de quelqu'un d'autre, il peut rediriger le deuxième utilisateur vers quelque chose qui ressemble à un programme et qui est malintentionné. Les ACLs sur les raccourcis doivent empêcher l'accès écriture aux utilisateurs avec moins de pouvoirs que ceux qui utilisent les raccourcis. Notez que les raccourcis qui apparaissent sur le bureau Windows NT et dans le menu démarrer sont généralement sûrs car ils sont stockés dans le répertoire profiles qui par défaut est privé. Vous pouvez aussi prévenir les utilisateurs de créer des raccourcis seulement dans l'arborescence de leur répertoire personnel et de désactiver l'accès écriture publique pour cet arbre.

Protéger les Extensions Standards

Windows NT conserve une correspondance (mapping) entre le noms des extensions de fichiers (comme ".TXT") et les programmes que le système doit appeler quand les utilisateurs font certaines actions (comme ouvrir ou imprimer) une icône avec cette extension. Ce simple mapping sert à tous les utilisateurs et ne devrait contenir que des programmes sûrs et dont les fichiers exécutables sont correctement protégés par des ACL.

Par défaut, le pseudo groupe INTERACTIVE, qui contient tous les utilisateurs qui peuvent se connecter localement sur l'ordinateur, peuvent modifier ou ajouter des entrées dans ce mapping en utilisant le menu "Affichage…Propriétés" sur le Poste de Travail. C'est une opportunité potentielle de spoofing. Windows NT garde ce mapping dans la Base de Registres sous la clé:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Classes
```

qui par défaut permet au groupe INTERACTIVE d'avoir l'accès "Modifier". En remplaçant ce groupe par un autre qui contient uniquement les utilisateurs de confiance vous éliminez cette menace.

Notez que les exécutables peuvent être lancés à partir des lignes de commandes sans distinction d'extension (qui est generalement.EXE) c'est pourquoi essayer d'enlever l'accès à une application en la renommant est futile. Comptez à la place sur les ACL des fichiers.

La partie *Système de Fichier & ACL du Registre* prescrit les paramètres d'accès affinés pour la clé Classes.

Définir des Extensions Standards

Même des applications légitimes peuvent réaliser des actions sensibles ou inattendues et peuvent être des opportunités pour le spoofing. Par exemple, les fichiers *.REG contiennent des scripts qui font que REGEDIT ajoute des entrées dans la base de Registres (qui est sujette aux permissions d'ACL). L'action par défaut "ouvrir" pour ces fichiers est d'appeler la fonction "import" de REGEDIT pour modifier automatiquement la Base de Registres.

L'utilisateur, quant à lui, voit seulement une petite fenêtre confirmant que la base de Registres a été mise à jour.

Conseils:

Niveaux 1 & 2:

- Nous *recommandons* que vous désactiviez les actions pour les fichiers portant l'extension .REG, et toutes celles que vous estimez pouvoir présenter les mêmes risques. Au Niveau 2, nous *recommandons* que vous désactiviez toutes les extensions, excepté celles qui sont opérationellement nécessaires et celles que vous estimez être dignes de confiance.

Retirer le "R" des Fichiers Programmes

C'est une excellente pratique que d'enlever la permission "R" des fichiers programmes exécutables (quoique évidemment, pas "X"). Ceci empêche les utilisateurs de copier le programme et d'utiliser leur propre version. Alors qu'un utilisateur ne peut accroître ses capacités en faisant de la sorte, la copie ne sera peut-être pas aussi fortement protégé que l'original et donc représente une menace de spoofing potentielle. Aussi, les programmes consultent souvent le répertoire du programme quand ils cherchent des DLL et copient un fichier programme dans un autre répertoire peut offrir une menace de spoofing. (Notez, toutefois, que le gestionnaire de bureau Windows NT ne peut déterminer l'icône pour de tels programmes, et affiche un icône par défaut. Ceci produit aussi beaucoup d'échecs de tentatives de lecture pour les sites qui auditent les échecs en Lecture, bien qu'ils puissent désactiver l'audit en lecture sur ces fichiers.)

Conseils:

Niveaux 1 & 2:

- Nous *recommandons* que vous enleviez l'accès "R" de tous les fichiers exécutables.

Explorateurs Internet

Le spoofing peut provenir de sources distantes. La menace populaire la plus puissante vient des explorateurs WWW qui chargent facilement et de façon transparente des programmes à partir des pages Web et les exécutent. Bien qu'au-delà de la portée de notre étude, de telles menaces d'applications sont importantes et dangereuses.

Spoofing de DLL

Le spoofing de DLL est un des plus insidieux sur Windows NT. Une Bibliothèque de liaison dynamique (Dynamic Link Library : DLL) est un module objet logiciel lié à un programme bien que le programme est exécuté. Les DLL's ont des caractéristiques puissantes qui permettent aux programmes de partager le code commun les rendant plus facile à développer et plus efficaces, et sont largement utilisées sous Windows NT.

Le code DLL s'exécute dans le contexte de son programme hôte et ainsi il hérite de la totalité des capacités du programme qui l'utilise. Un spoofing de DLL fait qu'un programme habituellement digne de confiance (généralement exécuté par un administrateur consciencieux) va charger une DLL avec un cheval de Troyes à la place de la DLL légitime. Une fois que le Cheval de Troyes prend le contrôle, il peut faire tout ce que l'utilisateur peut faire à son insu.

Quand les programmes chargent des DLL, ils cherchent une suite de répertoires à la recherche de DLL. Il est important que les intrus ne puissent insérer une "fausse" DLL dans l'un de ces répertoires où la recherche peut la trouver avant une DLL légitime portant le même nom. Ce qui rend plus confus ce problème est que les différentes méthodes de recherche utilisent des séquences de répertoires différents.

Les opportunités de spoofing DLL sont inhérentes aux méthodes que l'algorithme de lien de DLL utilise pour trouver le fichier qui contient la DLL. (Ces fichiers ont généralement le suffixe standard “.DLL”.) L'algorithme de lien cherche dans de nombreux endroits en fonction de la situation, mais on peut les grouper en trois grandes catégories:

- **Répertoire Programme**: C'est le répertoire qui contient les fichiers exécutables du programme.
- **Répertoire Système**: Une arborescence système censé être bien protégé , comme %SYSTEMROOT% (généralement “C:\WINNT”), ou ses sous-répertoires SYSTEM32.
- **Répertoire de travail**: C'est le répertoire de travail actuel du processus, qui peut être le répertoire dans lequel l'utilisateur est entré avant d'exécuter le programme, ou un répertoire dans lequel le programme s'est placé de lui-même. C'est le seul des trois qui ne puisse être protégé car ce peut être n'importe lequel des répertoires dans lequel l'utilisateur a navigué.

Le cas problématique se produit quand l’algorithme cherche le répertoire de travail pour trouver des fichiers DLL. Pour spoofer un utilisateur, on peut insérer une DLL malintentionnée dans un répertoire que l'utilisateur pourra utiliser comme répertoire de travail. Le fichier DLL doit avoir le même nom qu'une DLL légitime utilisée par le programme qui serait normalement sûre. Au lieu de se lier à la vraie DLL, l’algorithme va chercher la fausse DLL à la place. Il est très simple pour une DLL malintentionnée de générer un nouveau processus qui s'exécute avec les capacités totales de l’administrateur, et alors diriger les demandes vers la vraie DLL à laquelle l'on est censé accéder. (Les détails sont un peu au-delà de notre propos.)

La sécurité se retrouve limité par le fait que l'utilisateur exécutant un programme ne connaîtra peut-être pas lui-même le répertoire de travail du programme, étant donné que le programme configurera peut-être le répertoire. Même un utilisateur consciencieux qui cherchera à éviter les répertoires non protégés n'a que peu de façons de savoir quand le programme est dans l'un d'eux.

Les DLL chargées dans le répertoire du programme ne sont pas des menaces sérieuses car elles devraient être aussi bien protégées que le fichier lui-même. (ils ne devraient pas pouvoir être « en écriture » ou remplacés par des utilisateurs douteux.) Le répertoire Système est aussi présumé sûre en assumant le fait que ses ACLs sont correctement mises en place et en accord avec nos indications. La précaution principale dans ces deux cas est que les fichiers DLL soient aussi protégés que les programmes qui s y réfèrent.

Le système peut aussi utiliser le chemin de recherche pour des DLL, mais seulement après que les autres options possibles soient épuisées.

La clé de la base de Registres “KnownDLLs”:

```
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\
     SessionManager\KnownDLLs
```

définit un ensemble de DLL que le système charge au démarrage. Une liste d'exemple de cette clé:

```
advapi32=advapi32.dll
comdlg32=comdlg32.dll
crtdll=crtdll.dll
DllDirectory=Systemroot\System32
gdi32=gdi32.dll
```

Le système consulte le répertoire %SYSTEMROOT%\SYSTEM32 en premier (un Répertoire Système) pour des entrées KnownDLLs. La seule exception est une DLL 32-bit chargée dynamiquement par un programme grâce la fonction d'API LoadLibrary, qui ignore KnownDLLs. (Notez la valeur de “DllDirectory” dans KnownDLLs. Ceci est non documenté et nous conseillons de ne pas la modifier à moins que vous ne sachiez vous en servir.)

Une DLL appelée par une DLL dans KnownDLLs est aussi considérée comme une Known DLL. Donc, vous avez seulement besoin d’inclure les « racines » des arborescences DLL appelantes dans KnownDLLs. Malheureusement, il est difficile pour un administrateur de connaître cette hiérarchie d'appel.

Il est compliqué de choisir des endroits pour installer les DLL car il y a différents algorithmes pour des DLL 16-bit et 32-bits, qui diffèrent aussi dans leur traitement au niveau de l'entrée de la base de Registres KnownDLLs. Les cas suivants sont des endroits sûrs pour les DLL:

- Des DLL 32-bit installées de manière sûre dans le répertoire programme.
- Les DLL nommées dans KnownDLLs contenues dans le répertoire SYSTEM32, excepté quand il y a des DLL 32-bit chargées grâce à LoadLibrary.
- N’importe quelle DLL installée de manière sûre est chargée grâce à LoadLibrary par un chemin complet explicite. Ce sont généralement ceux dans le répertoire racine du système.

A cause du problème lié à LoadLibrary, il n'y a pas de solutions absolues contre le spoofing DLL. La liste suivante est au moins une base pour la sécurité des DLL. toutefois, elle peut aussi provoquer de considérable changements et ne devrait pas être appliquée à la légère.

- Toutes les DLL chargées dans le même répertoire que leurs applications sont en sécurité tant que leurs ACLs les protègent de la modification ou du remplacement.
- Placez tous les fichiers DLL du répertoire SYSTEM32 dans KnownDLLs.
- Déplacez toutes les autres DLL dans le répertoire SYSTEM32 et ajoutez-les dans KnownDLLs. Malheureusement, cela peut produire des erreurs sur les programmes qui utilisent ces DLL, bien que vous aurez généralement un message sur le fait qu'une DLL d'un certain nom n'a pu être trouvée.
- Scannez régulièrement le système pour les fichiers avec l'extension .DLL en dehors du répertoire SYSTEM32 ou du répertoire d'une application reconnue.

Malheureusement, les DLL chargées grâce à LoadLibrary qui n'utilisent pas de chemins absolus sont une faiblesse qu'un intrus visera souvent.

Pour plus d’information, voir [KBase] Q164501, “INFO: Windows NT Uses KnownDLLs Registry Entry to Find DLLs,” et la fonction d'API Win32 “LoadLibrary”.

Conseils:

Niveaux 1 & 2:

A ce stade aucune pratique pour prévenir le spoofing DLL semble suffisamment achevé pour être recommandée. Toutefois, les sites de Niveau 2 devraient prendre en considération les précautions cités plus haut comme une base pour leur propre politique de limitation du spoofing de DLL.

19. Responsabilités et Pratiques de l'utilisateur

Les utilisateurs sont en partie responsables de surveiller leur propre environnement et celui des groupes dont ils sont membres. Vous devriez créer des stratégies de site que tous les utilisateurs appliqueraient. Soulignons les points suivants à inclure dans la politique générale des utilisateurs. Il ne s'agit ici en aucune façon d'une liste exhaustive, mais, inclut des pratiques utilisateurs importantes en concordance avec ces conseils :

- Les utilisateurs doivent appliquer les procédures en vigueur pour le choix des nouveaux mots de passe, en particulier ce qui concerne le choix d'une combinaison aléatoire de caractères pour ce dernier.
- Ils doivent garder leur mot de passe confidentiel et ne pas l'écrire. Si les utilisateurs sont plus susceptibles d'écrire les mots de passe longs, malgré vos conseils, il peut être intéressant de leur spécifier une manière de protéger leurs mots de passe écrits.
- Ils ne doivent jamais utiliser leur mot de passe Windows NT pour une application nécessitant un mot de passe ou un autre système d'exploitations, en particulier DOS, Windows et Windows 95, et Macintosh.
- Les utilisateurs devraient entrer leur mot de passe seulement dans un scénario qui initie la connexion avec la séquence CTRL+ALT+DEL, en particulier : logon et logout, modification de leur mot de passe, et le verrouillage de la station. La seule exception est de se connecter à un partage distant sous un autre compte ce qui requiert la saisie du mot de passe correspondant au compte en question.
- Les utilisateurs ne devraient pas stocker de mots de passe dans des fichiers du système, tels que des fichiers batch ou des scripts de démarrage, spécialement le mot de passe de login Windows NT. Alors que ces fichiers peuvent en théorie rester confidentiels à l'utilisateurs, ils représentent un risque majeur et constituent une pratique dangereuse.
- Les utilisateurs devraient toujours verrouiller leurs stations avec la séquence CTRL+ALT+DEL lorsqu'ils laissent leur station libre s'il existe la moindre chance que d'autres utilisateurs utilisent la station à des fins malveillantes.
- Les utilisateurs devraient s'assurer que l'écran de veille avec verrouillage automatique qu'aurait éventuellement installé l'Administrateur reste activé. (Reportez-vous à la technique pour cacher la page d'économiseur d'écran du Panneau de Configuration dans la section *Fichiers de Stratégie Système*.)
- La plupart des applications ne sont pas programmées spécifiquement pour les ACLs de Windows NT. Pour éviter certains problèmes potentiels, les "documents" devraient conserver l'ACL qu'ils auraient s'ils étaient nouvellement crées dans le même répertoire. Si vous avez besoin d'affiner l'ACL sur un certain fichier, ajustez l'ACL sur le répertoire qui le contient ou déplacez le vers un autre répertoire où les fichiers ont, par défaut, l'ACL en question. (Voir le sujet "Applications et ACLs" dans [Sutt96], pages 102-104.)
- Les utilisateurs doivent garder à l'esprit que lorsqu'ils déplacent ou copient des fichier ou des répertoires, les nouvelles copies peuvent dans certains cas conserver leur ACL originale et dans d'autres cas être re-protégés conformément au répertoire dans lequel ils sont copiés ou déplacés. Dans le doute, il peut être utile de confirmer la nouvelle ACL. (Reportez-vous au sujet "Copie et Déplacement" dans [Sutt96], pages 98-100.)
- Les utilisateurs ne doivent pas importer de programmes non approuvés au sein de leur système. Les utilisateurs qui auraient ce droit devraient comprendre les pratiques pour

conserver ces programmes en sécurité, principalement en s'assurant que d'autres ne peuvent pas modifier les fichiers exécutables du programme, ainsi que les DLL. Ils doivent aussi protéger les fichiers de données qui n'ont pas à être modifiés par les autres utilisateurs.

- Il existe de nombreuses techniques contre le spoofing que les utilisateurs peuvent utiliser (voir *Spoofing*). Alors que cela serait fastidieux pour les utilisateurs que de suivre toutes les règles, un certain nombre nécessite une attention particulière :
  - Les utilisateurs ne devraient jamais double-cliquer sur une icône sauf s'ils savent sur quoi cela renvoit. Le conseil le plus avisé serait "Dans le doute, n'ouvrez, ne lancez ou ne cliquez pas sur une icône".
  - Les utilisateurs devraient garder les programmes personnels et les fichiers batch dans des répertoires sous leur contrôle où les autres utilisateurs ne peuvent ajouter, modifier ou remplacer ces fichiers.
  - De la même manière, ils ne devraient ajouter de répertoires que dans votre variable d'environnement PATH où les autres utilisateurs ne peuvent ajouter, modifier ou remplacer des fichiers.
  - Les programmes à exécution automatique sur CD-Roms ne peuvent se lancer que losrque le CD est inséré ou que l'icône du lecteur est ouverte. Les utilisateurs devraient éviter d'utiliser des CD-Roms non vérifiés , et utiliser la touche SHIFT pour outrepasser l'exécution automatique, quand c'est activé, en cas de doute sur le contenu d'un CD-Rom. (Voir la section "Les programmes d'exécution automatique sur CD-ROM" dans *Spoofing*.)

20. Bibliographie

Les références suivantes sont des sources d'informations sur la sécurisation NT qui ont inspiré ou du moins ont été prises en compte pour la conception de ce guide (par ordre d'influence):

[Sutt96] *Windows NT Security Guide*, par Stephen A. Sutton, Addison-Wesley, ISBN 0-201-41969-6. Ecrit par l'auteur de la version originale de cette étude, il est à la base de plusieurs des techniques de ce document. Il s'agit d'un didacticiel sur les concepts de sécurité sous Windows NT et donne de nombreuses instructions pour sécuriser ce dernier.

[Maye96] *Less Well-Known Considerations for Configuring a Secure Windows NT System*, Frank L. Mayer, SAIC, 29 Mars 1996. N'est plus disponible. Il s'agit d'un document fait par l'un des évaluateurs C2 qui a été à la base de nombreuses études menés par la suite. Bien que ce document ne soit plus disponible (ou à jour), ses idées sont suggerées par ces conseils.

[Micr97] *Securing Windows NT Installation*, Microsoft Corporation, 10 Avril 1997. Disponible sur leur site Web: http://www.microsoft.com

[TFM] *Windows NT C2 Security Administrator's Guide*. Il s'agit du "Trusted Facility Manual" nécessaire pour des évaluations C2, mais à notre connaissance il n'est pas généralement disponible au public. Nous avons examiné une copie finale non datée.

[Navy97] *Secure Windows NT Installation Guide*, Department of the Navy, Space and Naval Warfare Systems Command, Naval Information Systems Security Office, PMW 161, Novembre 1997. Récemment édité et généralement disponible au public. Bien que n'étant pas créé pour un usage général, il contient des indications spécifiques pour installer Windows NT pour la U.S. Navy.

Les documentations et produits suivants furent utiles dans la formulation de ce guide:

[ConPln] *Concepts and Planning Guide*, Windows NT Server Manuals, version 4.0. Disponible sur le CD-Rom de distribution de Windows NT.

[KBase] Microsoft's *Knowledge Base*, disponible dans de nombreux forums, incluant [TchNet], [RKitW], [RKitS], et sur http://www.microsoft.com. Les références aux articles de la Base de Connaissance (Knowledge Base) sont données par leur numéro d'accès uniques, par exemple "Q164501," vous y accédez en utilisant les fonctions de recherche correspondantes.

[NetGd] *Networking Guide* dans [RKitS].

[NetSp] *Networking Supplement Manual*, Windows NT Server Manuals, version 4.0. Disponible sur le CD-Rom de distribution de Windows NT.

[RKitW] *Ressource Kit* Microsoft pour Windows NT Workstation 4.0. Il s'agit d'un produit commercial fournit sur un CD-ROM qui inclut de la documentation et divers outils. Il est typiquement inclut dans [TchNet].

[RKitS] *Ressource Kit* Microsoft pour Windows NT Server 4.0. Il s'agit d'un produit commercial fournit sur un CD-ROM qui inclut de la documentation et divers outils. Il est typiquement incus dans [TchNet].

[TchNet] Le service d'information *Technet* de Microsoft, disponible par abonnement et distribué mensuellement sur CD-Rom. Les références à des articles de Technet sont données par leurs titres étant donné que vous pouvez utilisez le système de recherche intégré aux Technets

---

Nous avons pris en considération plusieurs ouvrages commerciaux concernant la sécurité Windows NT dans la préparation de ce guide :

[Micr94] *Windows NT 3.5 Guide for Security, Audit, and Control*, Microsoft Press, ISBN-1-55615-814-9.Une introduction générale à la sécurité sous Windows NT, mais l'ouvrage n'a pas été mis à jour pour les version récentes.

[Shel97] *Windows NT Security Handbook*, par Tom Sheldon, Osborne McGraw-Hill, ISBN 0-07-882240-8. Ce livre résume la documentation Microsoft et les autres concernant Windows NT, il s'agit d'une bonne référence générale concernant la sécurité sous Windows NT.

[Sutt96] *Windows NT Security Guide*. (Référence ci dessus.)

L'ouvrage suivant constitue une excellente (mais technique) présentation des principes de sécurité des réseaux:

[Kauf95] *Network Security: Private Communications in a Public World*, par Kaufman, Perlman, et Speciner, Prentice Hall, ISBN 0-13-061466-11.

Nous avons examiné d'innombrables sites Web et documents et voulions remarquer les suivants :

- *NT Security – Frequently Asked Questions*, une ***excellente*** collection d'informations sur la sécurité de Windows NT . La plupart des ces sites ont été examinés durant cette étude mais n'ont pas été spécifiquement nommés. Disponible sur:

  `http://www.it.kth.se/~rom/ntsec.html`

- *Problèmes de Sécurité Windows NT*, sur:

  `http://www.somarsoft.com.`

- *Exploits NT connus*, une base de données de "hacks" Windows NT disponible sur:

  `http://www.secnet.com/ntinfo/index.html`

- Documentation des produits de ISS, Inc., disponible sur:

  `http://www.iss.net/eval/manual/nt/index.html`

- *Final Evaluation Report, Microsoft, Inc., Windows NT Workstation and Server*. Il s'agit du rapport final de la commission d'évaluation C2 . Alors qu'il ne fournit aucun conseil de configuration, il constitue un excellent traité sur la structure de sécurité de Windows NT. Ce document *peut* être obtenu via le National Computer Security Center, Ft. Meade, MD.

- *Department of Defense Trusted Computer System Evaluation Criteria*, CSC-STD-001-83, Decembre 1985. Plus communément appelé “Orange Book,” ce document définit les critères d’une évaluation C2. Cependant, il ne s'agit pas d'une lecture générale et n'est pas utile pour comprendre comment configurer Windows NT de façon sécurisée. Remarquons que C2 n'est absolument pas un guide opérationnel – il ne présente pas comment un système doit être configuré dans un environnement particulier quel qu'il soit.

Fin